12. Wahlperiode

Drucksache **12/7951**

HESSISCHER LANDTAG

11. 02. 91

Neunzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 1990
gemäß § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 11. Februar 1991 · Ausgegeben am 19. März 1991

Herstellung: Johannes Weisbecker, 6000 Frankfurt am Main · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 6200 Wiesbaden 1

INHALTSVERZEICHNIS

1.	**Zur Situation**	9
1.1	20 Jahre hessische Datenschutzgesetzgebung	9
1.1.1	Datenschutz: Funktionsbedingung der Demokratie	9
1.1.2	„Datenschutz als Menschenrecht" – Veranstaltung am 10. Oktober 1990 im Hessischen Landtag	9
1.1.3	Chancen der föderalen Gesetzgebung	10
1.2	EG-Richtlinie zum Datenschutz	11
1.2.1	Ziel und Anwendungsbereich	11
1.2.2	Offene Fragen und Regelungsdefizite	11
1.3	Das neue Bundesdatenschutzgesetz	13
1.3.1	Flickwerk	13
1.3.2	Unzulässige Einschränkung der Kontrollbefugnisse des Bundesdatenschutzbeauftragten	14
1.3.3	Verfassungswidriger Eingriff in die Kontrollkompetenz der Datenschutzbeauftragten der Länder	15
1.3.4	Die Novellierung: ein Provisorium	15
1.4	Kontakte mit Thüringen	16
1.4.1	Stasi-Akten	16
1.4.2	Organisatorische und materiellrechtliche Voraussetzungen des Datenschutzes in Thüringen	17
1.4.3	Beschäftigtendaten	17
1.5	Regelungsaufgaben des Landesgesetzgebers	17
1.5.1	Hessisches Verfassungsschutzgesetz	17
1.5.2	Strafverfahren	18
1.5.3	„Aktenöffentlichkeit" im Umweltschutz	19
1.5.4	Änderungen des HDSG	19
1.6	Spektrum der Fälle	19
2.	**Europäische Gemeinschaft: Richtlinienentwürfe zum Datenschutz**	20
2.1	Neue Regelungsvorschläge	20
2.2	Hintergründe	20
2.3	Regelungsziele	21
2.4	Harmonisierung „nach oben"	21
2.5	Übermittlung ins Ausland	21
2.6	Weiteres Verfahren	22
3.	**Personaldatenverarbeitung**	22
3.1	Beihilfe für Angehörige eines Beamten	22
3.2	Prüfung von Beihilfeanträgen durch das Rechnungsprüfungsamt	23
3.3	Novellierung der Hessischen Beihilfenverordnung und der Verwaltungsvorschrift zur Durchführung der Beihilfenverordnung	24
4.	**Sozialverwaltung**	25
4.1	Köpenickiade im Kreisjugendamt	25
4.2	Beschlagnahme von Jugendamtsakten	25
4.3	Unnötig detaillierte Erziehungsberichte	26
5.	**Gesundheit**	26
5.1	Prüfungen der klinischen Krebsregister in den Städtischen Kliniken Darmstadt und Kassel sowie dem Universitätsklinikum Gießen	26
5.1.1	Funktion der klinischen Krebsregister	26
5.1.2	Datenschutz-Gesamtkonzept für die klinischen Krebsregister	27
5.1.3	Prüfungsergebnisse	28
5.2	Gesundheits-Reformgesetz – Auseinandersetzungen um die Angabe der Diagnose auf dem Krankenschein	31

6.	**Schulen**	32
6.1	Überprüfung der Notengebung einzelner Lehrer	32
6.1.1	Zulässigkeit der Kontrollen	32
6.1.2	Informationsansprüche der Betroffenen	33
6.2	Elternbefragung des Kultusministeriums im Lahn-Dill-Kreis	33
6.2.1	Fragebogen und Erhebungsverfahren	33
6.2.2	Umstrittene Zuständigkeit	33
6.2.3	Unnötige Verarbeitung personenbezogener Daten	34
6.2.4	Verletzung der Informationspflichten	34
6.2.5	Zweifel des Kultusministeriums am Personenbezug	35
6.2.6	Behandlung im Landtag	35
6.3	Richtlinien für den Datenschutz in Schulen	35
6.3.1	Notwendigkeit schulspezifischer Datenverarbeitungsregelungen	35
6.3.2	Inhalt der Richtlinien	36
6.3.3	Verzögerungen	38
7.	**Polizei**	38
7.1	Abschließende Novellierung des HSOG	38
7.1.1	Ausweitung der polizeilichen Befugnisse	38
7.1.2	Bewertung des § 16 HSOG	38
7.2	Erkenntnisanfrage über einen Sozialhilfebetrüger	40
7.3	Verbreitung von Informationen aus Homosexuellen- Publikationen durch Polizeidienststellen	40
7.3.1	Folgen eines Aufrufs	40
7.3.2	Datenverarbeitung der hessischen Polizeibehörden	41
7.4	Änderung des Anhörungs- und Vernehmungsbogens der Polizei	41
7.5	Polizeiliche Vorgangsverwaltung und Kriminalakten	42
8.	**Gesetz über das Landesamt für Verfassungsschutz**	42
8.1	Systematischer Ausgangspunkt	43
8.2	Aufgabenbeschreibung	43
8.3	Befugnisregelung	43
8.3.1	Erhebung von Daten über „Verdächtige" und „Unbeteiligte"	43
8.3.2	Akten- und Registereinsichtsrecht	44
8.3.3	Einsatz nachrichtendienstlicher Mittel	44
8.4	Zeitliche Begrenzung der Datenspeicherung	44
8.5	Datenaustausch zwischen dem Landesamt für Verfassungsschutz und anderen Behörden	44
8.6	Auskunftsregelung	45
9.	**Justiz**	45
9.1	Der „gläserne" Staatsanwalt	45
9.2	Prozeßkostenhilfe	46
10.	**Meldebehörden: Übermittlungen an öffentlich-rechtliche Stellen zu fiskalischen Zwecken**	47
11.	**Kommunen: Ratsinformationssysteme**	48
11.1	Funktion und Modellprojekte	48
11.2	Die Hessische Gemeindeordnung als Zugriffsrahmen	48
11.3	Stand und weiteres Verfahren	49
12.	**Umweltschutz**	49
12.1	Datenschutzregelungen im Hessischen Abfallwirtschafts- und Altlastengesetz	49
12.2	Einsichtsrecht in Umweltakten	49
13.	**Informationsrechte des Bürgers**	50
13.1	Auskunftsverhalten der Sicherheitsbehörden	50

13.1.1 Polizei ... 50
13.1.2 Landesamt für Verfassungsschutz ... 50
13.2 Benachrichtigung nach § 18 Abs. 2 HDSG ... 51
13.2.1 Ziel ... 51
13.2.2 Fehlentwicklung ... 51
13.2.3 Notwendigkeit einer Gesetzesänderung ... 51

14. ISDN (Integrated Services Digital Network) ... 55
14.1 Berichtsantrag der SPD-Fraktion ... 55
14.2 ISDN-fähige Anlagen ... 55

15. Datensicherheit ... 56
15.1 Datensicherheit durch technische und organisatorische Maßnahmen ... 56
15.2 Unverschlossene Staatskasse Wiesbaden ... 57
15.2.1 Mängel: 57
15.2.2 Forderungen: ... 57
15.3 Entsorgungskonzepte ... 58
15.4 Viren ... 58
15.5 Benutzerkontrolle bei DV-Anwendungen: Probleme der Passwortverwaltung ... 59
15.5.1 Dokumentation von Verfahrenspasswörten ... 60
15.5.2 Nutzung von Standardfunktionen ... 60
15.5.3 Gestaltung von Anmeldeprozeduren ... 61
15.5.4 Forderungen an die technische Realisierung einer Passwortverwaltung ... 61
15.5.5 Dokumentation von Passworten ... 62

16. Bilanz ... 62
16.1 Zusammenlegung von Meldeamt und Ausländerbehörde (18. Tätigkeitsbericht, Ziff. 2.5) ... 62
16.2 Sicherheitsbehörden ... 63
16.2.1 Aufhebung der Grenzkontrollen zwischen einigen EG-Ländern – Zusatzübereinkommen zum Schengener Abkommen (18. Tätigkeitsbericht, Ziff. 3.1, 17. Tätigkeitsbericht, Ziff. 1.3) ... 63
16.2.2 Die Datei ADOS der Verfassungsschutzämter (18. Tätigkeitsbericht, Ziff. 5.2) ... 64
16.3 Ausländerzentralregister (18. Tätigkeitsbericht, Ziff. 8) ... 64
16.4 Personaldatenverarbeitung ... 64
16.4.1 Hessisches Personalinformationssystem – HEPIS (16. Tätigkeitsbericht, Ziff. 8.2.2) ... 64
16.4.2 Unzulässiger Umgang mit Personalakten (18. Tätigkeitsbericht, Ziff. 9.1.2) ... 65
16.4.3 Automatisierte Verarbeitung von Lehrerdaten (18. Tätigkeitsbericht, Ziff. 9.1.3) ... 65
16.5 Post und Rundfunk ... 65
16.5.1 Neue Datenschutzverordnungen nach dem Poststrukturgesetz (18. Tätigkeitsbericht, Ziff. 16.2.3.1) ... 65
16.5.2 Kontrollbefugnis beim Hessischen Rundfunk (18. Tätigkeitsbericht, Ziff. 18.11) ... 65
16.6 Statistik ... 66
16.6.1 EG-Statistikverordnung (18. Tätigkeitsbericht, Ziff. 3.2) ... 66
16.6.2 Volkszählung 1987 (18. Tätigkeitsbericht, Ziff. 18.7) ... 66
16.6.3 Änderung des Mikrozensusgesetzes (14. Tätigkeitsbericht, Ziff. 5.3.2) ... 67

16.6.4 Hochschulstatistikgesetz
(18. Tätigkeitsbericht, Ziff. 10.2.2) 68

17. Materialien 68

17.1 20 Jahre Datenschutz in Hessen – eine kritische Bilanz. (Rede des Hessischen Datenschutzbeauftragten Prof. Dr. S. Simitis in der Veranstaltung am 10. Oktober 1990 im Hessischen Landtag zum 20. Jahrestag der Verabschiedung des ersten Hessischen Datenschutzgesetzes) 68

17.2 Berichte des Hessischen Datenschutzbeauftragten und Bericht der Landesregierung zu den Äußerungen des Innenministers Milde im Plenum des Hessischen Landtags am 24. Oktober 1990 75

17.2.1 Bericht des Hessischen Datenschutzbeauftragten vom 9. Oktober 1990 auf Beschluß des Hauptausschusses vom 25. Oktober 1990 (zur Veröffentlichung bestimmte Fassung des Berichts vom 8. November 1990) 75

17.2.2 Bericht der Landesregierung vom 14. November 1990 zu dem Beschluß des Hauptausschusses vom 8. November 1990 betreffend den Umgang mit Informationen, die aus Telefonüberwachungsmaßnahmen gewonnen wurden, innerhalb der Landesregierung 82

17.2.3 Bericht des Hessischen Datenschutzbeauftragten vom 19. November 1990 auf Beschluß des Hauptausschusses vom 8. November 1990 84

17.3 Beschlüsse und Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz 88

17.3.1 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Bundesdatenschutzgesetz vom 22./23. März 1990 und zum Bundesverfassungsschutzgesetz 88

17.3.2 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis 89

17.3.3 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zur Einrichtung eines Arbeitskreises EG 90

17.3.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 27. Juni 1990 zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität 91

17.3.5 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes 91

17.3.6 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes 92

17.3.7 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund und Ländern 93

KERNPUNKTE DES 19. TÄTIGKEITSBERICHTS

1. Der Landesgesetzgeber hat 1990 konsequent seine Bemühungen fortgesetzt, den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil von 1983 formuliert hat, Rechnung zu tragen: Mit der am 1. Januar in Kraft getretenen abschließenden Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und dem neuen Gesetz über das Landesamt für Verfassungsschutz hat der hessische Gesetzgeber zwei weitere wichtige Datenverarbeitungsbereiche der Landesverwaltung besonders geregelt.
   Die Ergänzung zu der im Dezember 1989 verabschiedeten Novelle des HSOG hat für den Datenschutz freilich nicht nur Verbesserungen gebracht. Die Vorschrift über den Einsatz von V-Leuten und verdeckten Ermittlern (§ 16) ist eindeutig verfassungswidrig (Ziff. 7.1).
   Das am 29. Dezember 1990 größtenteils in Kraft getretene Gesetz über das Landesamt für Verfassungsschutz ist deutlich besser als das jüngst verabschiedete Bundesverfassungsschutzgesetz und die vorliegenden Gesetzentwürfe verschiedener Bundesländer. Es weist jedoch auch eine Reihe von Defiziten auf. Zu den schwerwiegendsten Mängeln zählen der Verzicht auf die dringend notwendige Neubestimmung der Aufgaben des Verfassungsschutzes und auf eine den jeweiligen Aufgabengebieten des Verfassungsschutzes entsprechende Regelung der Datenverarbeitung (Ziff. 8.).
2. In krassem Gegensatz zu den Bemühungen des Landesgesetzgebers um mehr und besseren Datenschutz steht die Haltung des Bundesgesetzgebers. Das neue Bundesdatenschutzgesetz vom 20. Dezember 1990 bleibt nicht nur weit hinter den neuen Landesdatenschutzgesetzen zurück, sondern schränkt außerdem in verfassungswidriger Weise die Kontrollkompetenz der Datenschutzbeauftragten der Länder ein (Ziff. 1.3.3). Darüber hinaus fehlen bis heute in so zentralen Bereichen wie der Strafprozeßordnung Datenschutzregelungen (Ziff. 1.5.2).
3. Die Diskussion um die öffentliche Bekanntgabe von Informationen aus einem legal abgehörten Telefongespräch durch den früheren hessischen Innenminister Milde darf nicht versanden. Sie muß vielmehr zum Anlaß genommen werden, zu klären, in welchem Umfang ohne oder nur nach erfolgter Rücksprache bei der zuständigen Staatsanwaltschaft die Polizei und ihre Aufsichtsbehörde auf personenbezogene Daten aus strafrechtlichen Ermittlungsverfahren zugreifen darf (Ziff. 1.6 und 17.2).
4. Die von der EG-Kommission dem Ministerrat vorgeschlagene Richtlinie für den Datenschutz in den EG-Ländern ist trotz einiger Mängel ein wichtiger und bemerkenswerter Schritt in Richtung auf ein Europa der Bürger (Ziff. 1.2 und 2.).
5. Die „Verseuchung" von Personal Computern mit sog. „Virus- Programmen", die Daten löschen oder verändern, ist zu einem akuten Problem geworden. Die Verwaltung ist, allen gegenteiligen Behauptungen zum Trotz, derartigen Angriffen auf ihre Datenbestände jedoch keineswegs hilflos ausgeliefert. Es gibt durchaus technische und organisatorische Schutzmöglichkeiten – sie müssen nur genutzt werden (Ziff 15.4).
6. Zu den Grundvoraussetzungen des Datenschutzes zählt, daß der Betroffene Auskunft über seine bei den Behörden gespeicherten Daten verlangen kann. Der hessische Gesetzgeber hat dies inzwischen auch für die Daten der Polizei und des Verfassungsschutzes anerkannt. Bislang ist die Bereitschaft der Sicherheitsbehörden, den Betroffenen Auskunft über ihre gespeicherten Daten zu gewähren, höchst unterschiedlich. Während die Polizei recht großzügig verfährt, gibt das Landesamt für Verfassungsschutz nur sehr restriktiv Auskunft (Ziff. 13.1).
7. Die Hessische Beihilfenverordnung zwingt Angehörige eines Beschäftigten im öffentlichen Dienst, die Krankheitskosten erstattet haben wollen, zur unnötigen Offenbarung von Gesundheitsdaten. Dieser unhaltbare Zustand muß schnellstens beseitigt werden (Ziff. 3.1).
8. Wie der Fall „Peter Graf" zeigt, sind Mitarbeiter der Sozialbehörden oft völlig unzureichend über die besonderen Bestimmungen des Sozialdatenschutzes informiert (Ziff. 4.1).
9. Das für alle klinischen Krebsregister in Hessen gültige Datenschutzkonzept wird nur unzureichend eingehalten. Das haben mehrere Prüfungen gezeigt. Dabei wurde z.B. festgestellt, daß der Zugriff auf die im Register enthaltenen Patientendaten nicht – wie erforderlich – auf die jeweiligen behandelnden Fachabteilungen beschränkt war. Neben Mängeln bei der Erstellung und Weitergabe von Registerauswertungen zeigten sich außerdem Defizite bei den räumlichen, technischen und organisatorischen Datensicherheitsmaßnahmen (Ziff. 5.1).
10. Die Krankenkassen verlangen von den Ärzten, auf den Krankenscheinen die Diagnose zu vermerken. Dies ist unzulässig, da es dafür gegenwärtig keine Rechtsgrundlage gibt (Ziff. 5.2).
11. Die auf Anordnung des Kultusministeriums im Frühjahr 1990 im Altkreis Wetzlar durchgeführte Elternbefragung verstieß in vielfältiger Weise gegen das Datenschutzrecht. Die Befragung erfolgte nicht nur außerhalb des Kompetenzbereichs der Schulaufsichtsbehörde. Es wurden auch unnötig personenbezogene Daten erhoben und die Informationsrechte der Erziehungsberechtigten mißachtet (Ziff. 6.2).

1. Zur Situation

1.1
20 Jahre hessische Datenschutzgesetzgebung

1.1.1
Datenschutz: Funktionsbedingung der Demokratie

Am 30. September 1990 jährte sich zum zwanzigsten Mal der Tag der Verabschiedung des ersten Hessischen Datenschutzgesetzes. Wohl kaum ein anderes Landesgesetz hat die weitere Entwicklung nicht nur in der Bundesrepublik, sondern weit über ihre Grenzen hinaus so nachhaltig beeinflußt.

Für den hessischen Gesetzgeber gab es von Anfang an keinen Zweifel: Mit der Entscheidung für eine besondere, gesetzlich abgesicherte Verarbeitungsregelung sollte die Funktionsfähigkeit einer demokratischen Gesellschaft garantiert werden. Nicht anders hat es dreizehn Jahre später das Bundesverfassungsgericht gesehen. Beide, das Gericht und der Hessische Gesetzgeber, betrachten mithin einen konsequenten Datenschutz als eine der wichtigsten legislativen Aufgaben in einer Gesellschaft, die sich aus der Fähigkeit und der Bereitschaft der einzelnen Bürgerinnen und Bürger legitimiert, sich an gesellschaftlichen und politischen Entscheidungsprozessen selbst zu beteiligen und diese durch die eigene Reflexion und Meinungsbildung mitzutragen. Eben deshalb hat sich der Hessische Gesetzgeber bereits 1970 geweigert, nur die Verwertung ganz bestimmter Daten zu regeln, vielmehr gerade vor dem Hintergrund der durch die Automatisierung ermöglichten jederzeitigen Nutzung jedweder Daten für beliebig neudefinierbare Zwecke den Akzent einzig auf die Verarbeitung personenbezogener Daten gelegt. Aus dem gleichen Grund hat das Bundesverfassungsgericht nicht nur die Existenz „belangloser" Daten abgestritten, sondern zugleich ausdrücklich darauf hingewiesen, daß der Mangel an klaren, auch und vor allem den Bürgerinnen und Bürgern erkennbaren Verarbeitungsvoraussetzungen unweigerlich dazu führt, die Grundrechte auszuhöhlen, ja letztlich gegenstandslos werden zu lassen. Kurzum, für den Hessischen Gesetzgeber war die mit dem am 30. September 1970 verabschiedeten Datenschutzgesetz erstmals festgeschriebene Verpflichtung, sich bei der Datenverarbeitung nach bestimmten gesetzlich vorgegebenen Regeln zu richten, unmittelbarer Ausdruck zentraler verfassungsrechtlicher Grundsätze.

Der jüngste, sicherlich eindrucksvollste Beweis für die Richtigkeit dieser Überlegung läßt sich den Erfahrungen mit dem Demokratisierungsprozeß in Osteuropa entnehmen. In Ungarn etwa zählte die Erwartung, den Datenschutz in der Verfassung zu verankern und zugleich mit Hilfe einer eigens darauf zugeschnittenen gesetzlichen Regelung abzusichern, zu den ersten von der demokratischen Opposition in die Verhandlungen am Runden Tisch eingebrachten Forderungen. Aber auch sonst verlief die Entwicklung durchaus vergleichbar. Der Datenschutz geriet mehr und mehr zu einem der wichtigsten Ansatzpunkte der von den Bürgerbewegungen getragenen verfassungspolitischen Diskussion. In Wirklichkeit nur eine Wiederholung dessen, was sich bereits in Spanien und Portugal ereignet hatte. In beiden Ländern ist gerade die Bereitschaft, den Datenschutz durch ebenso restriktive wie verbindliche Verarbeitungsvorschriften zu garantieren, als manifestes Zeichen der Abkehr von totalitären Herrschaftsformen und des Übergangs zu einer demokratischen Gesellschaft gewertet worden. Sowohl in Spanien als auch in Portugal sind deshalb entsprechende Bestimmungen in die Verfassung aufgenommen worden. Ganz gleich freilich, ob man die damaligen Regelungsansätze oder die vor gar nicht allzu langer Zeit diskutierten Vorschläge im Rahmen der Verfassungsdebatten in Mecklenburg oder am Runden Tisch in Ost-Berlin nimmt, überall kehrt die Überzeugung wieder, daß die Manipulierbarkeit des einzelnen so lange eine reale Gefahr bleibt, wie sich der Zugriff auf Information zu seiner Person an ihm vorbei vollzieht und die Verarbeitung nicht von vornherein auf gesetzlich festgelegte Zwecke beschränkt ist. Anders ausgedrückt: Der Weg in eine Gesellschaft, welche die Freiheit des einzelnen auch und gerade als Recht begreift, anders zu sein, und in genau dieser Entwicklung des einzelnen zu einer selbständigen Person, die beste Voraussetzung für seine Mitwirkung an den gesellschaftlichen und politischen Entscheidungsprozessen sieht, führt über den Datenschutz.

1.1.2
„Datenschutz als Menschenrecht" – Veranstaltung am 10. Oktober 1990 im Hessischen Landtag

So gesehen sprach alles dafür, an den zwanzigsten Jahrestag der Verabschiedung des ersten Hessischen Datenschutzgesetzes mit einer am 10. Oktober 1990 im Hessischen Landtag vom Landtagspräsidenten gemeinsam mit dem Hessischen Datenschutzbeauftragten durchgeführten Veranstaltung zu erinnern, die ganz dem Thema „Datenschutz als Menschenrecht" gewidmet war. Und ebenso selbstverständlich erschien es, den Rückblick auf die Pionierjahre des Datenschutzes sowie die Bilanz der seitherigen Entwicklung mit einer Diskussion über die Bedeutung der informationellen Selbstbestimmung für den politischen Umbruch in Osteuropa zu verbinden, an der sich neben dem Präsidenten des ungarischen Verfassungsgerichtes, Professor László Sólyom, Dr. Hartmann, Mitglied des Rostocker Bürgerkomitees und Datenschutzbeauftragter für den Bezirk Rostock, Professor Dmitrij Tschereschkin, Forschungsdirektor am Institut für Angewandte Systemanalyse der Akademie der Wissenschaften in Moskau und der stellvertretende Direktor der Rechtsabteilung des Europarates Dr. Frits W. Hondius beteiligten.

Die Ausgangslage für eine Regelung, die das Recht des einzelnen anerkennt, selbst über den Umgang mit den seine Person betreffenden Daten zu entscheiden, ist, darüber waren sich alle Diskussionsteilnehmer einig, denkbar günstig. Die Reflexionen über die Notwendigkeit gesetzlicher Vorschriften sind keine abstrakten Spekulationen, sondern die zwingende Folge eigener, jahrelanger Erfahrungen mit einer staatlichen Verwaltung, die von den Bürgerinnen und

Bürgern eine grenzenlose Offenheit ebenso verlangte wie sie für sich eine kaum noch zu überbietende Geheimhaltung reklamierte. Der politische Umbruch hat zudem viele der osteuropäischen Staaten veranlaßt, sich um eine möglichst enge Verbindung mit dem Europarat zu bemühen. Keine andere internationale Organisation hat sich aber so konsequent für den Datenschutz eingesetzt wie der Europarat. Sowohl das Übereinkommen zum Schutz des Menschen bei der automatischen Datenverarbeitung vom 28. Januar 1981 als auch die zahlreichen seither verabschiedeten Empfehlungen haben die internationale Entwicklung maßgeblich beeinflußt, wie sich zuletzt an der Auseinandersetzung über das Schengener Abkommen deutlich gezeigt hat (vgl. 18. Tätigkeitsbericht, Ziff. 3.1.2; Ziff. 16.2.1 dieses Berichtes).

Und doch klangen in den einzelnen Diskussionsbeiträgen Zweifel und Skepsis immer wieder an. Schon deshalb, weil mit dem politischen Umbruch der Druck entfallen ist, den die Präsenz einer ebenso allmächtigen wie allgegenwärtigen staatlichen Bürokratie ausgeübt hat. Dafür sind mehr denn je die ökonomischen Sorgen in den Vordergrund gerückt. Je nachhaltiger sich aber die Aufmerksamkeit darauf konzentriert und alle Bemühungen verständlicherweise auf eine Verbesserung der wirtschaftlichen Lage abzielen, desto weniger dringlich erscheint die gesetzliche Absicherung noch so zentraler mit der Verwirklichung der Bürgerrechte verbundener Forderungen. Hinzu kommt eine wachsende Zahl von Einwänden, die genaugenommen symptomatisch für eine wiedererstarkende staatliche Bürokratie sind. Von der Notwendigkeit, über ein Höchstmaß an Information gerade in einer Zeit des ökonomischen und politischen Aufbaus zu verfügen, ist ebenso die Rede, wie von der wertvollen Hilfe, die manches der bestehenden Register nach wie vor leisten könnte, oder gar der Funktionsfähigkeit der staatlichen Verwaltung, die ohne die Möglichkeit gefährdet wäre, auf bewährte Datensammlungen zurückzugreifen. Schließlich gilt es nicht zu vergessen, daß, so wichtig gesetzliche Vorschriften auch sein mögen, sie so lange riskieren, dekoratives Beiwerk zu bleiben, wie die Betroffenen selbst nicht im Datenschutz eine Regelung sehen, die ihren ureigensten Interessen dient, deren Erfolg deshalb ganz entscheidend von ihrer Bereitschaft abhängt, die eigene Passivität zu überwinden und sich zuvörderst selbst kritisch mit den an sie gerichteten Informationsansprüchen auseinanderzusetzen. Wo es aber als schlicht selbstverständlich betrachtet wurde, etwa das statistische Geheimnis ausschließlich den aggregierten Daten vorzubehalten, die individuellen Angaben dagegen jeder Behörde für ihre Zwecke ohne weiteres zur Verfügung zu stellen, oder, fast noch grotesker, private Anschriften und Telefonnummern jederzeit erfragt werden konnten, Adressen und Telefonanschlüsse der Behörden aber grundsätzlich geheimzuhalten waren, fällt es verständlicherweise schwer, die Prioritäten gleichsam umzukehren und die Rolle eines beliebig nutzbaren Informationsobjekts zugunsten einer primär durch die eigene Entscheidung bestimmten Informationsverwertung abzustreifen.

1.1.3
Chancen der föderalen Gesetzgebung

Der hessische Gesetzgeber hat freilich mit seiner Entscheidung vom 30. September 1970 nicht nur den Weg für die weitere Entwicklung der Datenschutzgesetzgebung gebahnt und zugleich durch die unmißverständliche Verknüpfung der Datenschutzvorschriften mit verfassungsrechtlichen Grundprinzipien den Maßstab bestimmt, dem fortan jede Verarbeitungsregelung genügen mußte. Was sich vielmehr bereits beim 1. HDSG klar abzeichnete, haben die 1978 erfolgte Novellierung und erst recht das 1986 verabschiedete 3. HDSG bestätigt: An den Datenschutzvorschriften lassen sich wahrscheinlich besser als an nahezu jeder anderen Regelung die Notwendigkeit aber auch die Chancen einer föderalen Gesetzgebung ablesen.

Ohne die zunächst von einem weiteren Land, Rheinland-Pfalz, aufgegriffene Initiative Hessens und die späteren immer wieder von der Landesgesetzgebung ausgehenden Impulse hätte der Datenschutz niemals seinen gegenwärtigen Stand erreicht. Nicht nur, weil der Bund 1976 ebenso wie bei der gerade abgeschlossenen Novellierung des Bundesdatenschutzgesetzes hinter den im Landesbereich akzeptierten Anforderungen zurückgeblieben ist, sondern auch, weil er immer wieder bemüht war, die Regelungskompetenz der Länder mit dem Ziel zu unterlaufen, den Datenschutz einzuschränken. So stellte sich 1976 der Bundesgesetzgeber im Unterschied zu der vom Hessischen Gesetzgeber vertretenen Position auf den Standpunkt, Aufgabe der Datenschutzbestimmungen könne es nur sein, den „Mißbrauch" bei der Verarbeitung personenbezogener Angaben zu verhindern und leistete damit über Jahre allen auf eine möglichst restriktive Anwendung des Datenschutzes bedachten Bestrebungen Vorschub. So gelang es 1990 nur gegen erhebliche Widerstände und erst vor dem Hintergrund der von den Ländern geübten Kritik, die Datenerhebung sowie die Verarbeitung in Akten zumindest für den öffentlichen Bereich buchstäblich in letzter Minute in die Novellierung des BDSG einzubeziehen. So hat es der Bundesgesetzgeber anders als der Hessische Gesetzgeber abgelehnt, eine uneingeschränkte Verarbeitungskontrolle zu garantieren und zugleich bestimmt, daß die für die Kontrolle durch den Bundesbeauftragten vorgesehenen Einschränkungen auch dann gelten sollen, wenn die Aufsichtsfunktion durch die Landesbeauftragten wahrgenommen wird.

Kurzum, gerade die Geschichte der hessischen Gesetzgebung beweist: Zentralistische, im Namen einer falsch verstandenen Einheitlichkeit propagierte Bestrebungen haben den Datenschutz nicht gefördert, sondern im Gegenteil zu Regelungen geführt, die weit mehr zur Konservierung eingefahrener Verarbeitungspraktiken als zum Schutz der Betroffenen beigetragen haben. Nur solange der Landesgesetzgeber dezidiert auf seiner Kompetenz beharrt und ebenso entschieden alle mit ihr verbundenen Regelungsmöglichkeiten wahrnimmt, hat der Datenschutz eine echte Chance, die Verarbeitung personenbezogener Daten an Voraussetzungen zu binden, die nicht nur den Anforderungen des Grundgesetzes wirklich genügen, sondern auch mit einer sich zunehmend verfeinernden Verarbeitungstechnologie Schritt halten.

1.2
EG-Richtlinie zum Datenschutz

Bereits im Mai 1979 forderte das Europäische Parlament die Kommission auf, eine Richtlinie zur Harmonisierung des Datenschutzrechts vorzubereiten. Im März 1982 wiederholte es seinen Appell. Doch die Kommission zog es lange vor, möglichst ausweichend zu reagieren. Noch im August 1989 wiesen die Datenschutzbeauftragten der EG-Mitgliedsländer auf den Mangel an einschlägigen Vorschriften hin und verlangten eine möglichst rasche Intervention der Kommission (18. Tätigkeitsbericht, Ziff. 19.2.2). Inzwischen, genauer, seit dem 27. Juli 1990, liegt ein ganzes Vorschlagspaket vor, darunter auch der Entwurf einer Richtlinie „zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" (vgl. hierzu auch Ziff. 2 dieses Berichts).

1.2.1
Ziel und Anwendungsbereich

Dreierlei ist an dem Entwurf bemerkenswert: Die Kommission betrachtet, erstens, genauso wie zuvor der hessische Gesetzgeber und das Bundesverfassungsgericht, den Datenschutz als Konkretisierung der Grundrechte. Sie versteht deshalb ihre Vorschläge als Beitrag zu der von allen Gemeinschaftsorganen bekräftigten Verpflichtung, die Grundrechte der Gemeinschaftsbürger zu wahren, und damit als Baustein einer europäischen Grundrechtsordnung. Anders ausgedrückt: Ein „Europa der Bürger" kann nur vor dem Hintergrund verbindlicher Vorschriften über den Umgang mit personenbezogenen Daten entstehen.

So gesehen, ist, zweitens, der Regelungsspielraum der Gemeinschaft von vornherein beschränkt. Sie muß für die Regelung optieren, die den unter den gegenwärtigen Umständen bestmöglichen Datenschutz zu verwirklichen sucht. Konsequenterweise erklärt die Kommission ausdrücklich, sie strebe mit ihren Vorschlägen ein „hohes" Schutzniveau an. Gewiß, das Europaparlament hatte seinerzeit anders formuliert. Die Kommission sollte, so hieß es in der Entschließung vom 8. Mai 1979, für das „höchste" Schutzniveau sorgen. Wer jedoch dahinter einen Rückzug vermutet, übersieht den Sprachgebrauch der Gemeinschaft. Die Kommission hat mit ihrer Wortwahl nicht etwa die Bereitschaft zum Ausdruck gebracht, bei ihren Anforderungen an den Datenschutz nicht ganz so weit zu gehen wie es das Parlament wollte, sondern lediglich eine mittlerweile auch ansonsten, etwa beim Umweltschutz, verwendete Formel aufgegriffen. Signalisiert wird damit zweierlei: Zum einen, daß es nicht das Ziel der Regelung sein kann, sich an der Situation jener Mitgliedsstaaten zu orientieren, die noch immer über keinerlei Verarbeitungsregeln verfügen, mithin in die tastenden Anfänge des Datenschutzes zurückzufallen; zum anderen, daß die Gemeinschaftsregelung auch und gerade darauf bedacht sein muß, den Datenschutz fortzuentwickeln und sich infolgedessen nicht mit einer noch so gekonnten Mischung bestehender Vorschriften zufriedengeben darf.

Die Kommission beschränkt sich, drittens, allen gegenteiligen Mahnungen zum Trotz, keineswegs auf eine Regelung der Verarbeitung im „privaten" Bereich. Sie sieht, wie sinnlos, ja kontraproduktiv es wäre, etwa in Anbetracht der Verarbeitungsabläufe bei Arbeitnehmer-, Versicherten- und Patientendaten an der einst scheinbar so überzeugenden Gegenüberstellung von „privatem" und „öffentlichen" Bereich festzuhalten und bezieht zu Recht beide Bereiche in ihre Vorschläge ein. Wenn der Datenschutz wirklich ein Baustein der für ein „Europa der Bürger" erforderlichen rechtlichen Regelung sein soll, dann darf sich die Gemeinschaftsrichtlinie in der Tat nicht mit künstlichen Unterscheidungen abgeben, sondern muß im Gegenteil Verarbeitungsvoraussetzungen festlegen, die sich an der Verarbeitungsrealität orientieren.

1.2.2
Offene Fragen und Regelungsdefizite

1.2.2.1
Regelungskompetenzen des nationalen Gesetzgebers

So sehr die Überlegungen der Kommission zum Ziel und zum Anwendungsbereich der Richtlinie auch überzeugen, so wenig darf darüber übersehen werden, daß es im einzelnen durchaus eine Reihe von Punkten gibt, die sorgfältig überprüft werden müssen. Unklar ist beispielsweise, welche Regelungsmöglichkeiten dem nationalen Gesetzgeber verbleiben. Gewiß, der Entwurf enthält an einer Vielzahl von Stellen Formulierungen, die jedenfalls deutlich zu erkennen geben, daß die Kommission mit ihren Vorschlägen keine abschließende, jeglichen Gestaltungsspielraum des nationalen Gesetzgebers also ausschließende Regelung treffen möchte. Dennoch läßt sich dem Entwurf nicht klar entnehmen, ob die Kommission lediglich Mindeststandards für den gesamten Gemeinschaftsbereich festschreiben oder, wenn auch nur teilweise, verbindliche Regelungsgrenzen vorschreiben will. Um jedem Mißverständnis zuvorzukommen: Ganz gleich, wie man die Kommissionsvorschläge letztlich interpretiert, eine Folge haben sie mit Sicherheit: Soweit es um den Austausch personenbezogener Daten innerhalb der Gemeinschaft geht, kann eine Übermittlung so lange nicht verweigert werden, wie die von der Richtlinie aufgestellten Verarbeitungsgrundsätze eingehalten sind. Die Frage, ob nur Mindeststandards oder verbindliche Regelungsgrenzen angestrebt werden, spielt dagegen eine entscheidende Rolle, sobald die Verarbeitungsbedingungen im nationalen Raum und die Übermittlung in Drittländer im Vordergrund stehen. Dem von der Kommission ausdrücklich formulierten Ziel, ein „hohes Schutzniveau" anzustreben, kurzum, einen ebenso konsequenten wie effizienten Datenschutz sicherzustellen, kann nur eine Interpretation entsprechen, die in den Kommissionsvorschlägen lediglich eine Linie sieht, hinter die der nationale Gesetzgeber unter keinen Umständen zurückweichen darf. Die Vorschläge müssen mit anderen Worten aus seiner Sicht auch und vor allem Anreiz sein, den durch die Richtlinie erreichten Datenschutzstandard ständig weiter

zu verbessern. Nur unter dieser Bedingung kann es einerseits gelingen, die Folgen einer sich konstant verändernden Verarbeitungstechnologie aufzufangen und andererseits der Kommission Anregungen für die Fortschreibung ihrer Regelung zu vermitteln.

1.2.2.2
Notwendigkeit bereichsspezifischer EG-Regelungen

Die Richtlinie kann ferner lediglich eine erste Grundlage für die Auseinandersetzung mit den Verarbeitungsproblemen sein. Konkret: Ein wirklich wirksamer Datenschutz setzt mehr voraus als eine Reihe allgemeiner Grundsätze, so überzeugend sie im übrigen sein mögen. Vielmehr sind Regelungen notwendig, die gezielt auf die spezifischen Verarbeitungsprobleme bestimmter genau umschriebener Verarbeitungsbereiche eingehen. Erst dann läßt sich jenes Maß an Präzision erreichen, ohne das, wie die nationalen Erfahrungen nur zu gut zeigen, Umgehungsstrategien sich allzu leicht unter den breiten Mantel von Generalklauseln verstecken lassen. Sehr zu Recht hat deshalb die Kommission parallel zum Entwurf einer allgemeinen Richtlinie Vorschläge zum Datenschutz im Bereich der Telekommunikation vorgelegt. In die gleiche Richtung deuten bestimmte, im Entwurf enthaltene Regelungsansätze, deren offenkundiges Ziel es ist, die Entstehung bereichsspezifischer Vorschriften zu begünstigen. Die Kommission darf es freilich dabei nicht belassen. Sie muß möglichst bald Verarbeitungsregelungen für jene Bereiche vorlegen, in denen erfahrungsgemäß spezifische Datenschutzvorkehrungen besonders dringlich sind. Die Verarbeitung im Rahmen der Direktwerbung sowie im Versicherungs- und Kreditbereich sind wohl die wichtigsten Beispiele dafür.

1.2.2.3
Datenübermittlungen in Länder außerhalb der EG

Probleme gibt es auch beim „Export" personenbezogener Daten. Die Kommission weicht bei der Übermittlung personenbezogener Daten an Drittstaaten aus nicht ersichtlichen Gründen nicht nur von der ansonsten weitgehend übernommenen Regelung der Datenschutzkonvention des Europarates, sondern auch vom Grundsatz ab, den die nationalen Rechte bislang konsequent praktiziert haben. Die Zulässigkeit der Übermittlung soll nicht davon abhängen, ob im Empfängerland gleichwertige Datenschutzvorschriften bestehen. Der Entwurf gibt sich mit „angemessenen" Vorkehrungen zufrieden. Statt es also bei einer Formulierung zu belassen, die jedenfalls den für das Inland geltenden Datenschutzstandard einzuhalten sucht, zieht die Kommission eine Formel vor, die offenkundig darauf abzielt, geringere Anforderungen zu stellen, dadurch aber zwangsläufig das Risiko des Betroffenen erhöht.

Die Kommission spricht sich damit für eine Regelung aus, die den eigenen, ausdrücklich erklärten Intentionen offen zuwiderläuft. Wer sich so deutlich für ein „hohes Schutzniveau" einsetzt, darf keinen unterschiedlichen Maßstab anlegen, je nachdem, ob die personenbezogenen Daten innerhalb des Gemeinschaftsbereichs oder außerhalb seiner verarbeitet werden sollen. Er muß im Gegenteil alle ihm zur Verfügung stehenden Möglichkeiten dafür nutzen, um den angestrebten Schutz, soweit es nur irgendwie geht, auch dann zu gewährleisten, wenn sich die Verarbeitung in einem Drittland abspielt. Der Kommission sind dabei gewiß von vornherein Grenzen gesetzt. Sie hat dennoch, wie sich an den beiden Formeln zeigt, einen beachtlichen Spielraum. Die eigenen Regelungsprämissen lassen ihr allerdings keine Wahl. Sie muß sich für den Ansatzpunkt entscheiden, der den größtmöglichen Schutz gewährt, also eine „gleichwertige" Regelung fordern und sich nicht mit einer „angemessenen" begnügen. Der Austausch personenbezogener Daten wird dadurch ohne Zweifel erschwert. Die Drittländer haben es aber durchaus in der Hand, die Hindernisse abzubauen. Sie brauchen nur für entsprechende Datenschutzvorkehrungen zu sorgen. In Wirklichkeit keine allzu hohe Erwartung. Allein schon das Beispiel der Vereinigten Staaten beweist, wie weit die Datenschutzdiskussion auch in den Ländern fortgeschritten ist, die noch nicht über vergleichbare Regeln verfügen. Zudem gilt es nicht zu vergessen, daß sich der Europarat beim Datenschutz bewußt für eine offene Konvention entschieden und damit die Voraussetzungen für eine über die Mitgliedsstaaten hinausreichende Angleichung der Datenschutzanforderungen geschaffen hat. So gesehen, bietet die Forderung nach „äquivalenten" Datenschutzvorschriften einen doppelten Vorteil: Sie sichert nicht nur den einstweilen bestmöglichen Schutz der Betroffenen, vielmehr unterstützt und verstärkt sie zugleich die Bemühungen in den Drittländern, eigene Regelungen zu verabschieden.

1.2.2.4
Meldepflicht, Dateibezug, Zweckbindung

Darüber hinaus ist auf eine Reihe weiterer Regelungsdetails hinzuweisen, die genauso kritisch zu beurteilen sind, angefangen bei der Beschränkung des Anwendungsbereichs der vorgeschlagenen Regeln auf die Verarbeitung personenbezogener Daten in Dateien, über die mangelhafte, wenn nicht widersprüchliche Absicherung der Zweckbindung bis hin zu der durch die viel zu weit gefaßte Meldepflicht für Dateien heraufbeschworenen Gefahr einer Bürokratisierung des Datenschutzes. Die Kommission darf bei ihren Vorschlägen nicht die gerade beim Umgang mit den bisher geltenden nationalen Normen gemachten Erfahrungen außer acht lassen. Dann aber wird deutlich, daß mancher, lange Zeit für selbstverständlich gehaltener Regelungsansatz inzwischen seine Berechtigung verloren hat.

Eine umfassende Meldepflicht war beispielsweise ein zunächst durchaus willkommenes Mittel, um eine verläßliche Übersicht über Ausmaß und Gegenstand der Verarbeitung zu gewinnen. Allerdings hat sich relativ bald gezeigt, daß

eine derart extensiv konzipierte Verpflichtung die angestrebte Transparenz allein schon durch die Masse der Meldungen in Frage stellt. Konsequenterweise hat deshalb der schwedische Gesetzgeber die ursprüngliche Regelung mehr und mehr eingeschränkt. Ähnlich ist die französische Datenschutzkommission verfahren. Gezielte Anweisungen sollen einerseits dazu verhelfen, sorgfältig zwischen den verschiedenen speichernden Stellen zu unterscheiden und andererseits den Meldeprozeß soweit wie möglich auf wenige strikt formalisierte Informationen reduzieren.

Genauso überholt ist die Vorstellung, Datenschutzvorkehrungen könnten nur solange zum Zuge kommen, wie die personenbezogenen Angaben in Dateien verarbeitet würden. Wenn der Datenschutz wirklich gewährleistet werden soll, kann und darf es nicht weiter darauf ankommen, ob die Daten jeweils in Dateien, Akten oder sonstwo verarbeitet werden. Vielmehr muß die bloße Tatsache, daß personenbezogene Angaben verarbeitet werden, genügen, um die gesetzlich abgesicherten Schutzmechanismen auszulösen. Ganz in diesem Sinn bezieht das HDSG die Akten ein, eine Entscheidung, der sich mittlerweile der Bundesgesetzgeber im neuen Bundesdatenschutzgesetz wenigstens teilweise angeschlossen hat. Andere Mitgliedsstaaten der EG haben im übrigen einer Anknüpfung des Anwendungsbereichs ihrer nationalen Datenschutzgesetze an den Begriff der Datenverarbeitung statt an das Vorliegen einer „Datei" unmißverständlich den Vorzug gegeben.

Die Kommission legt schließlich zu Recht besonderen Wert auf eine strikt zweckgebundene Verarbeitung. Sie bekräftigt damit einen der sowohl von der Datenschutzkonvention des Europarates als auch vom Bundesverfassungsgericht formulierten Verarbeitungsgrundsätze. Schaut man freilich genau hin, stellt man alsbald fest, daß der Entwurf sich zwar dezidiert für eine Zweckbindung im öffentlichen Bereich ausspricht, bei einer Verarbeitung im privaten Bereich jedoch nicht ganz so klar vorgeht. Die Verpflichtung, sich durchweg nach einem auch und gerade dem Betroffenen erkennbaren Zweck zu richten, darf aber nicht unterschiedlich ausfallen, je nachdem ob eine Behörde oder ein privates Unternehmen auf personenbezogene Angaben zugreift. Sowohl die Transparenz der Verarbeitung als auch die Kontrollmöglichkeiten hängen entscheidend von der Zweckbindung ab. Wenn deshalb Interpretationen rechtzeitig vorgebeugt werden soll, die den Datenschutz in dem Augenblick nachhaltig einschränken, in dem die Verarbeitung im privaten Bereich stattfindet, dürfen die von der Richtlinie gewählten Formulierungen nicht voneinander abweichen.

1.2.2.5
Kontrollinstanz

Noch eine Bemerkung zur Kontrolle. Der Entwurf trennt zwischen der nationalen und der Gemeinschaftsebene. Für den nationalen Bereich gilt der Grundsatz: Einen wirksamen Datenschutz kann es ohne eine unabhängige, mit weitreichenden Rechten ausgestattete Kontrollinstanz nicht geben. Für den Gemeinschaftsbereich sieht der Entwurf lediglich eine aus Vertretern der nationalen Kontrollinstanzen bestehende, auf Konsultativaufgaben beschränkte „Gruppe" vor. So viel ist sicherlich richtig: Die Effizienz der Überwachung hängt entscheidend von der Nähe zur Verarbeitung ab. Jeder Versuch einer Zentralisierung kann überdies leicht zu einer die Kontrolle hemmenden Bürokratisierung führen. Insofern leuchtet es durchaus ein, die eigentliche Kontrollaufgabe bei den nationalen Instanzen zu lokalisieren. Die Bedeutung der auf der Gemeinschaftsebene vorgesehenen Instanz darf dennoch nicht unterschätzt werden. Ihr fällt nicht nur die Funktion zu, genau zu beobachten, wie sich die von der Richtlinie postulierten Datenschutzvorkehrungen im gesamten Gemeinschaftsbereich auswirken, also auch und vor allem Komplikationen und Hindernisse rechtzeitig auszumachen. Sie ist vielmehr zugleich der Angel- und Drehpunkt für schnelle Korrekturvorschläge und konkrete Initiativen zur Verbesserung der Gemeinschaftsvorschriften. Beides setzt aber genau das auch für die nationale Ebene vorgesehene Maß an Unabhängigkeit voraus. Der Entwurf zieht es dagegen vor, die „Gruppe" eng an die Kommission zu binden und deren Einfluß über eine Reihe organisatorischer Vorkehrungen sicherzustellen. Mag sein, daß es mit Rücksicht auf die bisherige Struktur sowohl der Kommission als auch der Gemeinschaft überhaupt schwerfällt, sich die Notwendigkeit der Existenz einer wirklich unabhängigen Instanz vorzustellen. Die tradierten Strukturen können freilich nicht der letzte und entscheidende Maßstab sein. Den Ausschlag kann wiederum nur das von der Kommission selbst gesetzte Ziel geben, ein „hohes Schutzniveau" zu gewährleisten. Anders ausgedrückt: Die Kommission muß es bei diesem Ziel auch dort belassen, wo der nationale Bereich überschritten wird und die Gemeinschaftsebene auf dem Spiel steht. Statt deshalb auf vorhandene Strukturen zu verweisen, gilt es, sich zu überlegen, wie Lösungen gefunden werden können, die den spezifischen Anforderungen des Datenschutzes genügen. Solange dieser Erwartung nicht entsprochen wird, es also an einer echten Unabhängigkeit der „Gruppe" fehlt, ist ihre Konsultativfunktion ebenso gefährdet wie die Chance, sich neben dem vom Entwurf gleichfalls vorgesehenen, aus Regierungsvertretern zusammengesetzten „Beratenden Ausschuß" als eigenständige Instanz etablieren und durchsetzen zu können.

1.3
Das neue Bundesdatenschutzgesetz

1.3.1
Flickwerk

Sieben Jahre nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 und vier nach der Verabschiedung des dritten HDSG ist die Novellierung des Bundesdatenschutzgesetzes endlich abgeschlossen. Das Ergebnis überzeugt, gelinde gesagt, nicht gerade. Kein Wunder, bedenkt man den mühsamen, von fortwährenden, bis in den Vermittlungsausschuß hineinreichenden Auseinandersetzungen und Korrekturen begleiteten Entstehungsprozeß. Der Grund liegt auf der Hand: Wer eine Vorlage erwartet hatte, die sich strikt an den Vorgaben des

Bundesverfassungsgerichts mit dem Ziel orientierte, den Datenschutz auch und gerade vor dem Hintergrund der seit 1976 gesammelten Erfahrungen konsequent auszubauen, konnte nur enttäuscht sein. Die Novellierungsvorschläge waren von Anfang an weit eher vom Wunsch getragen, möglichst wenig zu ändern, ja sogar manche für viel zu weitgehend empfundene Konzession rückgängig zu machen, als von der Einsicht in die evidenten, in den Tätigkeitsberichten der Datenschutzbeauftragten wieder und wieder genannten Datenschutzdefizite und in die Notwendigkeit, ein neues, der informationellen Selbstbestimmung wirklich entsprechendes Regelungskonzept zu entwickeln. So blieb nichts anderes übrig, als die parlamentarischen Verhandlungen zu nutzen, um immer wieder zu versuchen, datenschutzfreundlichere Regelungen durchzusetzen. Kein Zweifel, die Initiativen der Landesgesetzgeber, die Beschlüsse des Bundesrates, die Appelle der Konferenz der Datenschutzbeauftragten sowie die Kritik im Rahmen der zahlreichen Anhörungen haben viel bewirkt. Fast jede Vorschrift wurde neu redigiert. Wichtiger noch: Manche der zunächst für unabänderlich erklärten Positionen, wie etwa die kategorische Weigerung, die Akten oder die Erhebung in die Novellierung einzubeziehen, wurde zumindest teilweise aufgegeben.

Der Preis ist freilich hoch. Statt eines in sich geschlossenen, in allen Details sorgfältig abgestimmten Gesetzes ist ein Flickwerk entstanden. Vorschriften, die den Datenschutz verbessern, wechseln sich mit Regeln ab, die ihn einzuschränken suchen; auf scheinbar klare Positionsbestimmungen folgen Kompromisse, die den einmal eingenommenen Standpunkt verwässern, ja ins Gegenteil verkehren. So wendet sich der Gesetzgeber spät aber doch nicht ganz von der Vorstellung ab, Datenschutzvorkehrungen seien nur für den Mißbrauchsfall vonnöten, erleichtert jedoch zugleich beträchtlich die listenmäßige Übermittlung personenbezogener Angaben. So bemüht sich das Gesetz um eine möglichst exakte Regelung der Erhebung, soweit sie durch öffentliche Stellen erfolgt, beschränkt sich dagegen bei nicht-öffentlichen Stellen auf die letztlich nichtssagende Aufforderung, „Treu und Glauben" zu respektieren und sich im übrigen rechtmäßig zu verhalten.

1.3.2
Unzulässige Einschränkung der Kontrollbefugnisse des Bundesdatenschutzbeauftragten

Wohl am deutlichsten zeigt sich freilich die Ambivalenz der Novellierung bei den Bestimmungen über die Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz. Zur Erinnerung so viel: Das Bundesverfassungsgericht hatte in seiner Entscheidung von 1983 zum Volkszählungsgesetz ausdrücklich auf die Notwendigkeit einer unabhängigen Kontrolle hingewiesen und sie zu den unverzichtbaren Bestandteilen einer verfassungskonformen Verarbeitungsregelung gezählt. Insofern hätte alles dafür gesprochen, die noch bestehenden Kontrollschranken abzubauen und eine Regelung anzustreben, wie sie etwa das HDSG kennt. Das Gegenteil ist der Fall. Das Kontrollrecht des Bundesbeauftragten bleibt zwar äußerlich unangetastet, wird aber in ein kunstvoll geknüpftes Netz von Beschränkungen gehüllt, die allerdings nicht nur mit Hilfe der traditionellen Hinweise auf die „öffentliche Sicherheit und Ordnung" oder das „Wohl des Bundes" begründet werden. Die informationelle Selbstbestimmung wird vielmehr gleichsam gegen sich selbst gekehrt. Schließlich habe, so meint man, der Gesetzgeber mit seiner Intervention nichts anderes gewollt, als das Recht des einzelnen zu gewährleisten, selbst über den Umgang mit seinen Daten zu entscheiden. Wenn die Betroffenen also eine Überprüfung der zu ihrer Person verarbeiteten Angaben ablehnten, müsse es schlicht selbstverständlich sein, ihren Wunsch zu respektieren. Dementsprechend schließt das Gesetz eine Kontrolle etwa von Personalakten, Unterlagen, die im Zusammenhang mit einer Sicherheitsüberprüfung zusammengestellt wurden oder auch der Verarbeitung von Daten, die dem Arztgeheimnis unterliegen, in all den Fällen aus, in denen die Betroffenen der Kontrolle widersprochen haben.

Subtiler kann man es kaum machen: Unter dem Vorwand, den Betroffenen entgegenzukommen, wird die in ihrem Interesse unverzichtbare Kontrolle demontiert und in ein nutzloses Beiwerk verwandelt. Nicht von ungefähr haben die Datenschutzbeauftragten wieder und wieder darauf hingewiesen, daß die Kontrolle ihr Ziel, Aufschluß über den konkreten Verarbeitungsprozeß und dessen Mängel zu geben, solange nicht erreichen kann, wie nicht die Möglichkeit besteht, die gesamte Verarbeitungsaktivität einer einzelnen Behörde oder eines bestimmten Verwaltungszweiges einzubeziehen. Dem Datenschutzbeauftragten muß es insofern überlassen bleiben, festzulegen, ob sämtliche Unterlagen oder ein nur von ihm in Kenntnis der spezifischen Kontrollaufgaben näher definierter Ausschnitt der jeweils verarbeiteten Daten überprüft werden soll. Ganz in diesem Sinn ist auch die an die Adresse des Gesetzgebers gerichtete Forderung des Bundesverfassungsgerichts zu verstehen, die Voraussetzungen für eine wirksame Überprüfung zu schaffen. Wenn der Datenschutz wirklich die informationelle Selbstbestimmung und damit die Funktionsfähigkeit einer demokratischen Gesellschaft absichern soll, dann gilt es, auch und gerade für Kontrollbedingungen zu sorgen, die es erlauben, den Verarbeitungsprozeß in allen seinen Einzelheiten zu verfolgen. Nur dann kann die Überprüfung ihrer präventiven Aufgabe ebenso nachkommen wie Verstöße gegen die Datenschutzanforderungen rechtzeitig und erschöpfend aufdecken. Genau diese Möglichkeiten versperrt das Gesetz. Wer seine Folgen abschätzen will, braucht sich nur einen Augenblick lang die Kontrolle der Patientendaten eines Krankenhauses oder der Personalakten eines Ministeriums vorzustellen. Hält man sich an die gesetzliche Regelung, dann darf der Bundesbeauftragte mit seiner Prüfung erst beginnen, wenn die Betroffenen über ihr Widerspruchsrecht unterrichtet worden sind und sich auch entschieden haben, ob sie es ausüben möchten. Gewiß, der in der Abschlußphase gleich dreimal geänderte Wortlaut verwirrt. So soll der Bundesbeauftragte seine Kontrollbefugnis „unbeschadet" der Unterrichtung der Betroffenen über ihr Widerspruchsrecht ausüben können. Man kann dieser Formulierung entnehmen, daß der Bundesbeauftragte berechtigt ist, mit der Kontrolle ohne Rücksicht darauf zu beginnen, ob die Betroffenen bereits ausreichend informiert worden sind. Der Gesetzeswortlaut läßt sich aber auch umgekehrt dahingehend interpretieren, daß dem Bundesbeauftragten zwar prinzipiell eine Kontrollbefugnis zusteht, sie jedoch nur nach einer vorherigen Unterrichtung der Betroffenen ausgeübt werden darf, eine Auslegung, die sehr viel mehr den verarbeitenden Stellen entgegenkommt und deshalb bereits von ihnen offen favorisiert wird, obgleich

sie eindeutig den Aussagen der an den Arbeiten des Vermittlungsausschusses Beteiligten widerspricht. Das Gesetz scheint sich zudem mit einer „allgemeinen" Information zufriedenzugeben, erwartet aber, schaut man genauer hin, vom Betroffenen, „im Einzelfall" zu widersprechen, eine Feststellung, die, wie erste Erfahrungen zeigen, dazu verleitet, neben der generellen, gleichsam präventiven Unterrichtung, eine auf den je spezifischen Prüfungsfall bezogene Information zu verlangen. Der Widerspruch muß schließlich nicht der verarbeitenden Stelle, sondern der Kontrollinstanz gegenüber erklärt werden.

Kurzum, alle Korrekturen ändern nichts an der Möglichkeit einer Interpretation des Gesetzes, wonach der Prüfung stets eine gezielte, auf das Widerspruchsrecht zugeschnittene Information der Betroffenen vorauszugehen hat. Dem Bundesbeauftragten bliebe dann nichts anderes übrig, als zunächst etwa dem Ministerium oder dem Krankenhaus gegenüber seine Kontrollabsicht kundzutun, sich im Anschluß daran zu vergewissern, daß die Betroffenen ausreichend unterrichtet worden sind, um dann bis zu einem näher festzulegenden Zeitpunkt, über den wohl auch noch Einigkeit erzielt werden müßte, abzuwarten, ob einzelne Betroffene sich auf ihr Widerspruchsrecht berufen, eine Information, die ihn erst dazu befähigen würde, Umfang und Verlauf der Prüfung genau zu bestimmen. Das ohnehin überaus komplizierte Verfahren würde sich noch schwieriger gestalten, sobald die Zahl der Betroffenen besonders hoch ausfällt, weil beispielsweise sowohl Daten über die jetzigen als auch Angaben über frühere Patienten in die Kontrolle einbezogen werden sollen.

Von einer ernstzunehmenden, den Zielen des Datenschutzes entsprechenden Überprüfung könnte unter diesen Umständen schwerlich die Rede sein. Zudem: Spontane Kontrollen ließen sich gar nicht mehr durchführen, und zwar selbst dann, wenn sich der Bundesbeauftragte mit Vorfällen konfrontiert sehen sollte, die zu einer sofortigen Reaktion förmlich zwingen. Nichts anderes gilt für flächendeckende, auf die strukturellen Bedingungen etwa einzelner Krankenhausinformationssysteme ausgerichtete Kontrollen. Sie gehören in dem Augenblick der Vergangenheit an, in dem ein verläßlicher Überblick über die konkret verarbeiteten Datenmengen sowie die jeweiligen nur vom Einzelfall her überprüfbaren Verarbeitungsdetails nicht mehr möglich ist.

Von einer gesetzlichen Absicherung der auch und gerade vom Bundesverfassungsgericht unmißverständlich geforderten Kontrolle der Verarbeitung durch den Bundesbeauftragten läßt sich mithin in Anbetracht dieser Vorschriften nicht sprechen. Im Gegenteil, die Tätigkeit des Bundesbeauftragten wird beträchtlich erschwert, die Überprüfung entwertet. Das Gesetz überschreitet damit, vorsichtig ausgedrückt, die Grenze zu einer verfassungsrechtlich bedenklichen Regelung.

1.3.3
Verfassungswidriger Eingriff in die Kontrollkompetenz der Datenschutzbeauftragten der Länder

Zurückhaltende Formulierungen sind freilich spätestens dann vollends unangebracht, wenn es um die ebenfalls in der Novellierung enthaltene Aussage geht, die vorhin erwähnten, für die Kontrolle durch den Bundesbeauftragten geltenden Schranken müßten auch bei einer Überprüfung durch die Kontrollinstanzen der Länder beachtet werden. Die Novellierung greift mit dieser Vorschrift in eindeutig verfassungswidriger Weise in die Regelungskompetenz der Länder ein. Man kann sicherlich darüber streiten, ob es dem Bundesgesetzgeber ohne weiteres gestattet sein kann, die Datenschutzbeauftragten der Länder zu verpflichten, sich bei der Überprüfung der Anwendung von Bundesgesetzen in einer Weise zu verhalten, die ihren gesetzlich garantierten Befugnissen offen zuwiderläuft. Hingegen dürfte es keinen Zweifel geben, daß es dem Bundesgesetzgeber strikt untersagt ist, das Kontrollverfahren für die Verarbeitungsbereiche festzulegen, die ausschließlich der Regelungskompetenz des Landesgesetzgebers unterliegen. Anders ausgedrückt: Jeder Versuch des Bundesgesetzgebers, ihm aus welchem Grund auch immer als zu weitgehend erscheinende, im HDSG abgesicherte Kontrollbefugnisse des Hessischen Datenschutzbeauftragten auf dem Umweg über die Novellierung des BDSG zu verkürzen, ist verfassungswidrig. Die Landesregierung darf deshalb eine solche Regelung nicht reaktionslos hinnehmen.

Ebensowenig geht es an, sich mit der inzwischen offenkundigen Tendenz abzufinden, die in der Novellierung aufgezählten materiellen Kontrollschranken als Konkretisierung einer Regelungsprärogative des Bundes auszugeben, die dem Landesgesetzgeber jede Möglichkeit nimmt, für seinen Bereich eigene Vorschriften und damit genuines Landesrecht etwa für die Personalakten oder die Sicherheitsüberprüfung der Landesbediensteten zu formulieren. Auf dem Spiel steht deshalb nicht nur die Verpflichtung zu einer verfassungskonformen Datenschutzregelung, sondern genauso die Existenz- und Funktionsfähigkeit föderaler Gesetzgebung.

1.3.4
Die Novellierung: ein Provisorium

Selbst wenn man die Einschränkungen der Verarbeitungskontrolle ebenso wie etwa die widersprüchliche Erhebungsregelung oder die weitgehende Freigabe listenmäßig übermittelter Daten einen Augenblick beiseite lassen sollte, sprechen mindestens drei Gründe dafür, daß die längst fällige Reform des BDSG keineswegs mit der gerade verabschiedeten Novellierung abgeschlossen sein kann: Der Bundesgesetzgeber ist, erstens, mit seiner Regelung teilweise beträchtlich hinter den in einer Vielzahl von Landesgesetzen formulierten Verarbeitungsanforderungen zurückgeblieben. Der Druck, die mit der Novellierung getroffenen Entscheidungen zu überprüfen, wird deshalb, zumal vor dem Hintergrund der vom Bundesverfassungsgericht festgelegten Regelungsvorgaben, zunehmen.

Jedes Datenschutzgesetz hat, zweitens, bislang unter dem Vorbehalt einer sich rapide weiterentwickelnden Informations- und Kommunikationstechnologie gestanden. Die Novellierung hat sich allen Mahnungen zum Trotz kaum bemüht, den seit 1976 eingetretenen Veränderungen der Technologie Rechnung zu tragen und erst recht nicht versucht, ein hinreichend flexibles und offenes Regelungskonzept zu finden, das wenigstens mit den bereits absehbaren Entwicklungen einigermaßen Schritt halten könnte. Datenschutzvorschriften, die dieser Anforderung nicht genügen, verwirken sehr schnell ihren Geltungsanspruch.

Die Novellierung wird sich, drittens, sehr bald an den von der Europäischen Gemeinschaft postulierten Datenschutzvorschriften messen lassen müssen. Ein Vergleich mit den Kommissionsvorschlägen läßt jetzt schon erkennen: Die Gemeinschaft ist nicht bereit, die von der Novellierung gleichsam auf die Spitze getriebene Diskrepanz zwischen den Datenschutzanforderungen für Behörden und öffentliche Stellen einerseits und für private verarbeitende Stellen andererseits mitzumachen. Sie lehnt es, anders ausgedrückt, ab, den Datenschutz mehr und mehr als eine letztlich dem öffentlichen Bereich vorbehaltene Verpflichtung anzusehen und demzufolge die Verarbeitung personenbezogener Daten im privaten Bereich, soweit es nur irgendwie geht, freizugeben. Eben deshalb sieht der Kommissionsentwurf, anders als die Novellierung, beispielsweise gezielt davon ab, unterschiedliche Kontrollverfahren vorzuschreiben. Die Überwachung muß vielmehr nach der Vorstellung der Kommission in beiden Fällen völlig unabhängigen, mit klaren Eingriffskompetenzen ausgestatteten Instanzen anvertraut werden.

Hinzu kommt ein weiterer, für das Schicksal der Novellierung nicht minder wichtiger Gesichtspunkt. Sowohl das Volkszählungsurteil des Bundesverfassungsgerichts als auch die inzwischen im Rahmen der Landesgesetzgebung gesammelten Erfahrungen und die Tätigkeitsberichte der Datenschutzbeauftragten machen deutlich: Ein wirklich wirksamer Datenschutz läßt sich nur mit Hilfe bereichsspezifischer Regeln erreichen. Der Bundesgesetzgeber hat im öffentlichen Bereich die Bereitschaft dazu durchaus erkennen lassen, auch wenn längst angemahnte, besonders wichtige Regelungen, beispielsweise die Novellierung der Strafprozeßordnung oder gesetzlich abgesicherte Verarbeitungsvorkehrungen bei der Telekommunikation nach wie vor fehlen. Im privaten Bereich dagegen hat der Bundesgesetzgeber nicht einmal ansatzweise Konsequenzen aus den Berichten der Aufsichtsbehörden etwa zur Verarbeitung für Kredit- und Werbungszwecke gezogen. Aus der zumindest angekündigten Absicht, die Verarbeitung von Arbeitnehmerdaten zu regeln, ist bislang ebenfalls nichts geworden. Dennoch: In dem Maße, in dem der Gesetzgeber seiner Verpflichtung nachkommen sollte, den Datenschutz über bereichsspezifische Bestimmungen besser zu sichern, dürften die abstrakten und gerade deshalb mehrdeutigen Aussagen der Novellierung jedenfalls für die aus der Perspektive der Betroffenen wichtigsten Verarbeitungsbereiche an Bedeutung verlieren. Auch unter diesem Aspekt ist die Novellierung nicht mehr als ein Provisorium.

1.4
Kontakte mit Thüringen

1990 war auch ein Jahr intensiver, in Erfurt und Wiesbaden geführter Gespräche mit den thüringischen Bürgerbewegungen sowie den für den Aufbau des Landes zuständigen Stellen. Vor allem zweierlei stand dabei im Vordergrund: der weitere Umgang mit den Akten des Staatssicherheitsdienstes und die für eine Verwirklichung des Datenschutzes notwendigen organisatorischen und materiellrechtlichen Voraussetzungen.

1.4.1
Stasi-Akten

Die Unterlagen des Staatssicherheitsdienstes unterliegen mittlerweile den im Staatsvertrag getroffenen Bestimmungen und der Benutzungsordnung vom 17. Dezember 1990. Es kann keinen Zweifel daran geben, daß die Regelungskompetenz nicht bei den Ländern liegt. Eines ändert sich trotzdem nicht: Die Erfahrungen der einzelnen Bürgerkomitees bleiben ein entscheidender Ansatzpunkt für die Anwendung der Regelungen. Daß dabei Datenschutzfragen eine wichtige Rolle spielen, ist nicht weiter verwunderlich. Schließlich geht es bei der Aufarbeitung der Akten fast durchweg um personenbezogene Informationen. Insofern lassen sich gerade jene Regeln, die den Umgang mit personenbezogenen Daten zum Gegenstand haben, nicht einfach übersehen. Mehr als befremdlich sind dagegen die wiederholten Versuche, der Forderung nach einer möglichst intensiven Auseinandersetzung mit den sich aus den Akten ergebenden Informationen, den Datenschutz als zwar bedauerliche, aber kaum überwindbare Barriere entgegenzuhalten. Solche Behauptungen erinnern in fataler Weise an die Diskussion über den Zugang zu den Unterlagen aus der Zeit des Nationalsozialismus. Damals wie heute war man bestrebt, den Datenschutz zu instrumentalisieren, um einen Rückgriff auf die Unterlagen möglichst einzuschränken. Geschichte läßt sich aber auch nicht auf dem Weg über eine verfehlte Interpretation der Datenschutzvorkehrungen verdrängen. Spätestens seit der Verabschiedung der Archivgesetze hat kein Versuch eine Chance mehr, sich hinter den Datenschutz zu verschanzen.

Nicht minder vorsichtig gilt es gegenüber der pauschalen Übernahme einzelner Datenschutzbestimmungen zu sein. So mag es unter Datenschutzgesichtspunkten keinen Zweifel an der Notwendigkeit eines dem Betroffenen zustehenden, prinzipiell uneingeschränkten Auskunftsrechts geben. Auf den ersten Blick spricht viel dafür, bei den Akten des Staatssicherheitsdienstes ebenso zu verfahren. Die Entscheidung darüber, wie dieses Auskunftsrecht genau auszugestalten ist, ob es also beispielsweise einem uneingeschränkten Recht gleichkommt, die jeweiligen Akten einzusehen, darf nur unter Berücksichtigung der besonderen, die Informationserhebung begleitenden Umstände und der spezifischen Art und Weise der Verarbeitung in den Akten getroffen werden. Inwieweit sich unter diesen

Voraussetzungen die Forderung nach einem als Einsichtsrecht verstandenen Auskunftsrecht aufrechterhalten läßt, bleibt noch zu klären.

Mittlerweile hat eine weitere, scheinbar nicht mit der Aufarbeitung der Staatssicherheitsakten zumindest unmittelbar zusammenhängende, Frage mehr und mehr an Bedeutung gewonnen. Der Staatsvertrag bemüht sich, Regeln für jene inzwischen dem Sonderbeauftragten weitgehend übergebenen oder zumindest seiner Obhut anvertrauten Aktenbestände aufzustellen, die vor allem dank der rechtzeitigen Intervention der Bürgerkomitees vor einer Vernichtung bewahrt werden konnten. Längst steht aber fest, daß eine beträchtliche Zahl an Akten nicht zuletzt von früheren Angehörigen des Staatssicherheitsdienstes an die verschiedensten Interessenten veräußert worden sind. Der weitere Umgang mit diesen Akten kann aber nicht deshalb gleichgültig sein, weil sie sich nicht mehr in den vom Staatsvertrag angesprochenen Beständen befinden. Sie gehören genauso wie alle anderen Unterlagen zum Informationsmaterial, das ausschließlich nach den für die Akten des Staatssicherheitsdienstes bereits festgelegten oder noch vorzuschreibenden Bedingungen aufgearbeitet werden muß. Gerade deshalb kommt es ganz besonders darauf an, nicht nur eine Verpflichtung vorzusehen, die Unterlagen zurückzugeben, sondern sich auch zu überlegen, ob und welche Sanktionen für den Fall einer Verwendung vorgesehen werden müßten. Nur unter dieser Voraussetzung läßt sich die Gefahr zumindest eindämmen, daß Unterlagen, die sich vorzüglich für Manipulations- und Erpressungsversuche eignen, über Jahre hinweg beliebig genutzt werden.

1.4.2
Organisatorische und materiellrechtliche Voraussetzungen des Datenschutzes in Thüringen

Bei den Gesprächen über die organisatorischen und materiellrechtlichen Voraussetzungen des Datenschutzes haben vor allem drei Überlegungen im Vordergrund gestanden. Für Thüringen gilt, erstens, ebenso wie für die anderen vier „neuen" Länder nichts anderes als für die „alten" Länder: Es ist ausschließlich Sache des Landesgesetzgebers, die für seinen Kompetenzbereich notwendigen Datenschutzvorkehrungen zu treffen. So schwierig die Aufgaben auch sein mögen, vor denen die „neuen" Länder stehen, so wenig rechtfertigen sie eine verfassungsrechtlich unzulässige Verkürzung ihrer Regelungskompetenz. Daran ändern auch die im Staatsvertrag enthaltenen Übergangsvorschriften nichts. Sie sind nicht mehr als ein provisorischer Ausweg, der deshalb so schnell wie möglich den Entscheidungen des Landesgesetzgebers weichen muß. Der Landesgesetzgeber ist dabei, zweitens, auch wenn es zunächst seltsam klingt, in einer durchaus vorteilhaften Lage. Er kann von den Erfahrungen der „alten" Länder profitieren und den Gesetzgebungsprozeß sehr viel wirksamer gestalten. Anders und konkreter ausgedrückt: Er braucht den ebenso langen wie komplizierten Weg von den ursprünglich für ausreichend gehaltenen allgemeinen Datenschutzbestimmungen zu den inzwischen als unverzichtbar anerkannten bereichsspezifischen Vorschriften nicht nachzuvollziehen. Der Landesgesetzgeber hat vielmehr vor dem Hintergrund der mittlerweile klar umrissenen Problembereiche und der bereits bestehenden gesetzlichen Regelungen die Möglichkeit, parallel vorzugehen, also neben den allgemeinen Vorschriften auch die erforderlichen bereichsspezifischen Bestimmungen zu verabschieden. Der Vorteil liegt auf der Hand: Das Gesetzgebungsverfahren läßt sich vereinfachen. Die einzelnen Regelungen können zudem von Anfang an sorgfältig aufeinander abgestimmt werden. Weder die Gesetze über die einzelnen Sicherheitsbehörden noch etwa die für den Gesundheitsbereich geltenden Vorschriften bräuchten also nachträglich korrigiert zu werden. Für den Gesetzgeber müßte im Gegenteil feststehen: Eine Regelung der polizeilichen Tätigkeit etwa kann und darf nur in Zusammenhang mit den für diesen Bereich notwendigen Datenschutzvorkehrungen erfolgen und in gleichzeitiger Abstimmung mit den generellen Datenschutzvorschriften.

1.4.3
Beschäftigtendaten

Schließlich: Die angestrebte Privatisierung der staatlichen Betriebe darf nicht eine „Privatisierung" ihrer Informationsbestände zur Folge haben, jedenfalls soweit es um die Arbeitnehmerdaten geht. Das Arbeitsverhältnis war in der DDR Kristallisationspunkt einer Vielzahl von Informationen zur Person der einzelnen Arbeitnehmer, die weit über die jeweils im Zusammenhang mit der konkret übernommenen Tätigkeit erforderlichen Angaben hinausgingen. Die Betriebe verfügen insofern gegenwärtig noch über einen inzwischen eindeutig rechtswidrigen Informationsbestand. Ganz gleich deshalb in wessen Hand sie sind, jede Verwendung der davon betroffenen Daten ist unzulässig. Nur kann es nicht bei dieser Feststellung bleiben. Vielmehr gilt es, möglichst bald für eine Bereinigung der einzelnen Informationsbestände zu sorgen, alle Angaben also umgehend zu vernichten, deren Verarbeitung den im BDSG oder in den speziellen arbeitsrechtlichen Vorschriften formulierten Anforderungen widerspricht.

1.5
Regelungsaufgaben des Landesgesetzgebers

1.5.1
Hessisches Verfassungsschutzgesetz

Die Verabschiedung des dritten HDSG im November 1986 war der erste Schritt auf dem Weg zu einer den Anforderungen des Bundesverfassungsgerichts entsprechenden Gesetzgebung. Der Landesgesetzgeber hat seither diesen Weg konsequent weiter verfolgt. Das jüngste Beispiel dafür ist das Verfassungsschutzgesetz (vgl. auch Ziff. 8). Seine Geschichte ist in doppelter Hinsicht für die wachsenden Schwierigkeiten bezeichnend, denen sich alle Versuche ausgesetzt sehen, eine verfassungskonforme Verarbeitungsregelung sicherzustellen. Zum einen nimmt der Druck, die Entscheidung doch noch hinauszuschieben, in dem Maße zu, in dem sich der Landesgesetzgeber Verarbeitungs-

bereichen nähert, in denen sich Bundes- und Landesgesetze seit jeher ergänzen und der Bundesgesetzgeber zudem bislang jedenfalls die Akzente bestimmt hat. Als Begründung dient durchweg der Hinweis, man müsse eben erst einmal abwarten, welchen Weg der Bundesgesetzgeber gehen wolle. Die Folgen haben sich beim Verfassungsschutzgesetz besonders bemerkbar gemacht. Eigentlich gab es spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz im Dezember 1983 keinen Zweifel mehr: Das Verfassungsschutzgesetz gehört zu jenen Regelungen, die mit am schnellsten hätten revidiert werden müssen. Doch die von Tätigkeitsbericht zu Tätigkeitsbericht wiederkehrenden Mahnungen wurden stereotyp mit der Bemerkung zurückgewiesen, der Bundesgesetzgeber sei noch nicht so weit. Erst in dem Augenblick, in dem das Ende einer ohnehin reichlich bemessenen Übergangsfrist nahte und auch die Gerichte ihre Absicht erkennen ließen, weitere Verzögerungen nicht mehr hinzunehmen, änderte sich die Reaktion. Wie wenig stichhaltig das Argument einer gleichsam durch das Verhalten des Bundesgesetzgebers oktroyierten Wartefrist ist, hatte zudem das Land Bayern mit seiner Entscheidung deutlich demonstriert, eine Regelung ohne Rücksicht auf das Verhalten des Bundes zu treffen.

Zum anderen waren gerade die ersten Regelungsvorschläge typisch für die ebenfalls weit verbreitete Tendenz, die Aufforderung des Bundesverfassungsgerichts, den Datenschutz gesetzlich abzusichern, mehr und mehr von ihrem sachlichen Hintergrund zu lösen und unter rein formalen Gesichtspunkten zu betrachten. Genauer: Wenn sich das Gericht unmißverständlich dafür ausspricht, den Gesetzgeber einzuschalten, dann deshalb, weil damit nicht nur die jeweiligen Verarbeitungserwartungen offengelegt, sondern auch im einzelnen vor dem Parlament legitimiert und von diesem ausdrücklich gebilligt werden müssen. Nur unter dieser Voraussetzung läßt sich in der Tat das vom Bundesverfassungsgericht bekräftigte Ziel erreichen, die Verarbeitung personenbezogener Daten eben nicht als selbstverständlich hinzunehmen, sondern sie als besonders zu rechtfertigende Ausnahme zu betrachten und zu behandeln. Statt jedoch die Notwendigkeit einer legislativen Entscheidung zunächst und vor allem zum Anlaß zu nehmen, die eigenen Verarbeitungspraktiken kritisch mit dem Ziel zu überprüfen, die Verarbeitungserwartungen möglichst einzuschränken, wurde die Intervention des Gesetzgebers zunehmend in einen formalen Akt umgedeutet, der die bisherigen Verarbeitungsvorgänge ebenso wie neue Verarbeitungswünsche abdecken sollte.

Just diese, anfänglich durchaus vorhandene Tendenz hat sich in den parlamentarischen Beratungen nicht durchsetzen können. Im Gegenteil, die parlamentarischen Gremien haben nahezu jede der vorgeschlagenen Vorschriften eingehend diskutiert und sich fast durchweg für Regelungen entschieden, die den Datenschutz deutlich verbessern. Gewiß, nach wie vor gibt es Bestimmungen, die im Interesse eines wirksamen Datenschutzes anders hätten formuliert werden müssen. So richtet sich das Gesetz bei der Festlegung der Verarbeitungsbefugnisse nicht nach der jeweiligen, dem Verfassungsschutz zugewiesenen Aufgabe, sondern enthält eine globale und deshalb viel zu undifferenzierte Regelung. Dennoch: Ein Vergleich mit den vom Bundesgesetzgeber jüngst verabschiedeten Vorschriften oder auch den mittlerweile ebenfalls vorliegenden Landesgesetzen zeigt, wie sehr der Hessische Gesetzgeber seine Entscheidung einmal mehr als Verpflichtung verstanden hat, die Vorgaben des Bundesverfassungsgerichts in konkrete, auch und gerade die Situation der Betroffenen berücksichtigende Datenschutzvorkehrungen umzusetzen.

Man kann, ja man muß einwenden, daß die Entscheidung zu einem Zeitpunkt gefallen ist, zu dem eigentlich alles dafür gesprochen hätte, sich vor dem Hintergrund der politischen Entwicklung zunächst einmal darüber klarzuwerden, ob es bei den bisherigen Aufgaben des Verfassungsschutzes bleiben kann und wie seine Organisationsstruktur künftig aussehen muß, um erst dann die erforderlichen gesetzlichen Vorschriften zu formulieren. Nur darf man dabei nicht das Dilemma übersehen, vor dem der Gesetzgeber gestanden hat. Die Anforderung des Bundesverfassungsgerichts und das Ende der Übergangsfrist schränkten seinen Handlungsspielraum von vornherein ein. Er durfte weder die bisherige Regelung weiter hinnehmen noch konnte er weiter abwarten. So gesehen, gab es keine Alternative zur Verabschiedung eines neuen Gesetzes. Eines ändert sich trotzdem nicht, das Gesetz kann gerade wegen der im politischen Bereich eingetretenen Änderung nur eine provisorische Regelung sein. Gerade deshalb gilt es aber auch einmal mehr vor allen Bestrebungen zu warnen, dem Verfassungsschutz gleichsam als Kompensation für weggefallene Aufgaben polizeiliche Funktionen zu übertragen, etwa bei der Bekämpfung der organisierten Kriminalität. Ein konsequenter, wirklich ernstgenommener Datenschutz, setzt eine klare Trennung zwischen Polizei und Verfassungsschutz voraus. Wo sie mit welcher Begründung immer preisgegeben wird, führt die Aufgabenvermischung über kurz oder lang zur Preisgabe der für eine verfassungskonforme Regelung unentbehrlichen Zweckbindung der Verarbeitung zugunsten einer nicht mehr durchschaubaren und auch nicht mehr kontrollierbaren Verwendung der jeweiligen Daten.

1.5.2
Strafverfahren

Wesentlich komplizierter als beim Verfassungsschutzgesetz ist die Lage bei der Strafprozeßordnung. Die Regelungskompetenz des Bundes steht außer Frage. Ebensowenig läßt sich übersehen, daß der Bundesgesetzgeber die längst fällige Novellierung der StPO immer wieder hinausgeschoben hat. Darunter haben nicht zuletzt alle Bestrebungen deutlich gelitten, Datenschutzvorkehrungen für den Bereich der Sicherheitsbehörden gesetzlich festzulegen. Die der Sache nach notwendige Abstimmung mit den StPO-Vorschriften mußte unterbleiben, weil der Bundesgesetzgeber nach wie vor auf einer den Anforderungen des Bundesverfassungsgerichts offenkundig nicht entsprechenden Regelung beharrt, wie allein schon die Auseinandersetzung um die Zweckbindung im Rahmen einer Verarbeitung personenbezogener Daten nach den StPO-Bestimmungen zeigt. Sieben Jahre nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 kann zudem der Bundesgesetzgeber beim besten Willen keinen „Übergangsbonus" für sich in Anspruch nehmen. Der Landesgesetzgeber hat insofern keine Wahl: Er muß sich überlegen, wie sich die eigenen Möglichkeiten am besten ausschöpfen lassen, um rechtswidrige Verarbeitungen zu vermeiden.

1.5.3
„Aktenöffentlichkeit" im Umweltschutz

So wichtig freilich die gerade mit der immer noch ausstehenden Novellierung der StPO zusammenhängenden Fragen sind, sie dürfen nicht den Blick für die nach wie vor offenen, originären Aufgaben des Landesgesetzgebers versperren. Mit das beste Beispiel dafür ist neben den Datenschutzbestimmungen im Bereich des Umweltschutzes die Diskussion über die „Aktenöffentlichkeit". Der hessische Gesetzgeber hat sich zu keinem Zeitpunkt auf die ebenso falsche wie gefährliche Gegenüberstellung von Datenschutz und „Aktenöffentlichkeit" eingelassen, sondern von Anfang an klar zu erkennen gegeben, daß sowohl wirksame Datenschutzvorkehrungen als auch eine für die Bürgerinnen und Bürger möglichst transparente Verwaltung zu den Grundelementen eines an den Funktionsbedingungen einer demokratischen Gesellschaft orientierten Informationssystems zählen. Die Wissenschaftsklausel im HDSG ist ebenso ein Zeichen dafür wie die einschlägigen Bestimmungen des Archivgesetzes. Insofern ist es nur konsequent, die bislang punktuellen Ansätze fortzuentwickeln und jedenfalls die gerade aus der Perspektive der Bürgerinnen und Bürger wichtigsten Verwaltungsbereiche einzubeziehen. Die in diese Richtung zielenden Erwartungen der Europäischen Gemeinschaft sind Anlaß genug, nicht weiter abzuwarten.

1.5.4
Änderungen des HDSG

Mehr und mehr zeichnet sich allerdings noch eine ganz andere Aufgabe ab, nämlich die seit 1986 gewonnenen Erfahrungen zu nutzen, um bestimmte Vorschriften des HDSG zu korrigieren, die anders als ursprünglich erwartet, nicht dazu geführt haben, den Datenschutz zu verbessern. Der Tätigkeitsbericht weist in diesem Zusammenhang auf die Benachrichtigungspflicht hin (Ziff. 13.2). Sie ist vor dem Hintergrund der Einsicht in die Grenzen des Auskunftsrechts entstanden und sie bleibt der wichtigste Ansatz, um den Bürgerinnen und Bürgern einen möglichst verarbeitungsnahen Einblick in die Verwendung ihrer Daten zu vermitteln. Die Benachrichtigungspflicht kann aber vor allem aus zwei Gründen dieser Aufgabe gegenwärtig nicht genügen. Zum einen sind bestimmte, aus der Perspektive der Betroffenen besonders relevante Bereiche, wie etwa die Sozialverwaltung, von der Benachrichtigungspflicht ausgenommen aber nicht vom HDSG. Zum anderen ist die Gefahr groß, daß eine unterschiedslos gehandhabte Benachrichtigungspflicht eben nicht das Interesse der Bürgerinnen und Bürger weckt, sondern sie gerade in Anbetracht zunehmend formalisierter Mitteilungen am Sinn einer solchen Information zweifeln läßt. Die ursprüngliche Regelung kann deshalb nicht mehr aufrechterhalten werden. Sie muß Bestimmungen weichen, die es ermöglichen, die Benachrichtigungspflicht flexibel zu gestalten und auf einzelne, für die Betroffenen wirklich relevante Bereiche zu konzentrieren.

1.6
Spektrum der Fälle

Der Tätigkeitsbericht bringt wie jedes Jahr eine Reihe von Fällen, die entweder Verstöße gegen den Datenschutz illustrieren oder auf bestimmte, noch offene, regelungsbedürftige Datenschutzfragen hinweisen. Das Spektrum der Fälle ist auch diesmal breit. Probleme, die bei der Gewährung von Beihilfen entstehen (Ziff. 3), gehören ebenso dazu, wie etwa die Datenschutzanforderungen bei der Verarbeitung von Patientendaten in Krebsregistern (Ziff. 5.1), der Durchführung von Elternbefragungen (Ziff. 6.2), der Einrichtung von „Ratsinformationssystemen" (Ziff. 1.1), der Dokumentation bestimmter Vorgänge in den Kriminalakten (Ziff. 7.5) oder auch die inzwischen fast klassischen Fragen der Datensicherheit (Ziff. 15). Dabei zeigt sich nicht zuletzt, wie dringlich nach wie vor manche schon früher erhobene Forderung ist. Der Fall „Graf" (Ziff. 4.1) ist ein gutes Beispiel dafür. Sicher geht es auch um die Bedingungen, die im Interesse der Betroffenen erfüllt sein müssen, bevor sich ein Jugendamt überhaupt auf Fragen Dritter einläßt. Nur wäre es falsch, sich mit Überlegungen zufriedenzugeben, die lediglich das Verhalten des Jugendamtes betreffen. Zur Debatte steht weit mehr die Frage, ob es nicht Grenzen bei der Informationserhebung durch die Presse geben muß und wo sie zu ziehen sind. Auf die Notwendigkeit, sich damit auseinanderzusetzen, hatte bereits der 1988 vorgelegte 17. Tätigkeitsbericht (Ziff. 1.1.4) aufmerksam gemacht, allerdings in einem ganz anderen Zusammenhang, dem Aids-Test einer afrikanischen Asylbewerberin und der darauf folgenden Information der Presse. Der Hessische Justizminister hat kurz danach eine Reihe weiterer Aspekte der auf die Verarbeitung personenbezogener Daten durch die Presse zurückzuführenden Probleme aufgegriffen. Der Deutsche Juristentag hat sich ebenfalls damit beschäftigt. Mittlerweile hat auch der Presserat versucht, seine Richtlinien zu präzisieren. Noch fehlt es freilich an überzeugenden Antworten. Der Fall „Graf" zeigt, wie wichtig es ist, sie möglichst bald zu finden.

Wohl kein anderer Fall hat freilich im vergangenen Jahr so viel Aufsehen erregt, wie die mit Zitaten aus der Zusammenfassung eines Abhörprotokolls versehene Rede des früheren hessischen Innenministers Milde vor dem Landtag. Die beiden im Auftrag des Hauptausschusses erstatteten Berichte sind im Anhang des Tätigkeitsberichts (Ziff. 17.2.1 und 17.2.3) abgedruckt. Auch hier kommt es entscheidend darauf an, sich nicht mit Überlegungen zum konkreten Fall zufriedenzugeben, sondern die weit darüber hinausreichenden prinzipiellen Fragen nicht aus den Augen zu verlieren. Die Probleme, um die es dabei geht, werden am Ende des 1. Berichts ausdrücklich erwähnt. Auf zweierlei sei trotzdem noch einmal hingewiesen.

Zunächst: Alle Beteuerungen, Entscheidungen über den Umgang mit den im Rahmen eines Ermittlungsverfahrens verarbeiteten personenbezogenen Daten seien der Staatsanwaltschaft vorbehalten, müssen solange ebenso unrealistisch wie unglaubwürdig bleiben, wie nicht die Zugriffsmöglichkeiten der Polizei und ihrer vorgesetzten

Behörden eindeutig geklärt sind. Anders ausgedrückt: Wer immer noch behauptet, die Staatsanwaltschaft sei die „Herrin" des Verfahrens und damit den Eindruck eines unbedingten Vorrangs ihrer Entscheidung auch und gerade im Hinblick auf die konkret erhobenen Angaben erweckt, ist spätestens seit den jüngsten Erfahrungen widerlegt.

Ferner: Informationen, die aus einer Telefonüberwachung stammen, müssen im Hinblick auf Art. 10 Grundgesetz einer besonderen, ihre jederzeitige Lokalisierung durch die Staatsanwaltschaft garantierenden Regelung unterliegen. Nichts anderes darf übrigens dann gelten, wenn die hessischen Staatsanwaltschaften das Bundeskriminalamt einschalten. Die Staatsanwaltschaften müssen mit anderen Worten auch und gerade in diesem Fall die Möglichkeit haben, genau zu verfolgen, wie sich bestimmte Vorgänge innerhalb des Bundeskriminalamts abgespielt haben und ob ihre Vorgaben genau eingehalten worden sind. Nur unter dieser Voraussetzung hat das unter verfassungsrechtlichen Gesichtspunkten unabdingbare Vernichtungs- bzw. Löschungsgebot des § 100b Abs. 5 StPO eine reelle Chance beachtet zu werden.

So wenig sich jedoch bestreiten läßt, daß der Landesgesetzgeber und die Landesregierung einen großen Teil dieser Fragen regeln können, so sehr zeigt sich einmal mehr, daß eine verfassungskonforme Verarbeitung personenbezogener Daten ganz entscheidend von der Revision der Strafprozeßordnung abhängt. Jede weitere Verzögerung der Novellierung ist deshalb gerade vor dem Hintergrund der jüngsten Erfahrungen ein offener Verstoß gegen den verfassungsrechtlich gebotenen Datenschutz.

2. Europäische Gemeinschaft: Richtlinienentwürfe zum Datenschutz

2.1
Neue Regelungsvorschläge

„Ein „Europa der Bürger" kann ohne verbindliche, den Datenschutz im gesamten Gemeinschaftsbereich garantierende Verarbeitungsbedingungen nicht entstehen." So lautete die Quintessenz meiner Kritik im letzten Tätigkeitsbericht (Ziff. 1.3) an der langjährigen Untätigkeit der EG-Kommission im Bereich des Datenschutzes. Im Juli 1990 kam endlich der Startschuß für einschlägige gesetzgeberische Aktivitäten aus Brüssel. Bis dahin datierte die letzte nennenswerte Aktion vom Juli 1981; damals sprach die EG-Kommission die Empfehlung an alle Mitgliedstaaten aus, umgehend die Europaratskonvention zum Datenschutz vom Januar 1981 zu ratifizieren. Dieser Empfehlung sind aber bis heute nur sieben Mitgliedsländer – darunter auch die Bundesrepublik Deutschland – gefolgt, allerdings mit ganz unterschiedlichen Regelungskonzeptionen und -modellen.

Mit Schreiben vom 27. Juli 1990 hat die EG-Kommission nunmehr zwei Richtlinienvorschläge dem Rat der Europäischen Gemeinschaften zur Beschlußfassung zugeleitet (vgl. Bundesrats- Drucks. 690/90 vom 04.10.1990). Zum einen handelt es sich um einen „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" (im folgenden: „Datenschutzrichtlinienvorschlag" a.a.O., S. 9 bis 73). Zum anderen hat die Kommission einen „Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" vorgelegt (a.a.O., S. 80 bis 104).

2.2
Hintergründe

Die Motive für den Sinneswandel der EG-Kommission sind sicherlich vielfältig. Mitentscheidend war zweifellos das ständige Drängen der Datenschutzkontrollinstanzen, die „Datenschutzoasen" in der Gemeinschaft zu beseitigen und damit zu verhindern, daß der z.B. in Frankreich und der Bundesrepublik Deutschland vorhandene Schutzstandard durch Verlagerung der Datenverarbeitung in ein EG- Land ohne eigenes Datenschutzgesetz unterlaufen werden kann. Eine wichtige Rolle dürfte außerdem die Erklärung gespielt haben, die die Datenschutzbeauftragten der EG-Länder am 30. August 1989 im Rahmen der internationalen Konferenz der Datenschutzbeauftragten abgegeben haben (vgl. 18. Tätigkeitsbericht, Ziff. 19.2.2). Darin wird eine EG-Richtlinie auch wegen des Ausbaus der grenzüberschreitenden informationellen Zusammenarbeit (beispielsweise im Polizeibereich) und der zunehmend den Mitgliedsländern durch Gemeinschaftsrecht aufgegebenen Datenerhebungspflichten gefordert.

Ausschlaggebend für die Kommission war aber wohl letztlich die Furcht vor Behinderungen des „informationellen Binnenmarkts" durch divergierende nationale Datenschutzgesetze bzw. unterschiedliche Entscheidungen der Datenschutzinstanzen bei grenzüberschreitenden Datenübermittlungen. Als Warnung konnte in diesem Zusammenhang der „FIAT-Fall" dienen, in dem die französische Datenschutzkommission (CNIL) gegen eine Datenweitergabe der FIAT-Filiale in Frankreich an die Muttergesellschaft in Italien unter Hinweis auf die fehlende Datenschutzgesetzgebung im Empfängerland rechtliche Bedenken erhoben hatte.

2.3
Regelungsziele

Zielsetzungen und wesentliche Inhalte der Datenschutzrichtlinie hat die Kommission folgendermaßen zusammengefaßt: „Dieser Vorschlag der allgemeinen Richtlinie verfolgt das Ziel, in allen Mitgliedstaaten der Gemeinschaft ein gleichwertiges hohes Schutzniveau einzuführen, um die Hemmnisse für den Austausch von Daten abzubauen, der für das Funktionieren des Binnenmarktes unerläßlich ist. Dazu müssen die in dem Entwurf eines Richtlinienvorschlags genannten Grundsätze von den Mitgliedstaaten garantiert werden. Diese Grundsätze beziehen sich insbesondere auf die Bedingungen, unter denen eine Verarbeitung personenbezogener Daten rechtmäßig ist, die Rechte der betroffenen Person (Recht auf Unterrichtung, Auskunftsrecht, Recht auf Berichtigung, Einspruchsrecht usw.), die nötige Qualität der Daten (sie müssen richtig, nach Treu und Glauben, für bestimmte rechtmäßige Zweckbestimmungen gespeichert sein usw.), die Einsetzung einer Gruppe für den Schutz personenbezogener Daten, die die Kommission in Fragen des Datenschutzes berät. Der Entwurf des Richtlinienvorschlags gilt für den privaten wie für den öffentlichen Bereich, dessen Tätigkeiten in den Anwendungsbereich des Gemeinschaftsrechts fallen. Da jeder in jedem Mitgliedstaat bei der Verarbeitung personenbezogener Daten den gleichen hochwertigen Schutz genießen können wird, werden die Mitgliedstaaten die Freizügigkeit dieser Daten in der Gemeinschaft nicht mehr mit der Begründung des Schutzes der betroffenen Person einschränken können." (Bundesrats-Drucks. 690/90, S. 10).

Entscheidend ist der letzte Satz des Zitats. Auch wenn in der Begründung zum Richtlinienvorschlag auf das Engagement der Gemeinschaft für die Wahrung der Grund- und Persönlichkeitsrechte verwiesen wird, wichtiger erscheint der Kommission das Ziel, den freien Informationsfluß im künftigen Binnenmarkt abzusichern. Dazu werden den Mitgliedsländern verbindliche Vorgaben gemacht: Wer noch kein Datenschutzgesetz hat, wie etwa Belgien oder Italien, muß ein solches bis zum 1. Januar 1993 in Kraft setzen. Wer bereits ein Gesetz hat, muß dieses bis zu dem genannten Datum an die Regelungen der Richtlinie anpassen (Art. 31 Nr. 1 Datenschutzrichtlinienvorschlag).

2.4
Harmonisierung „nach oben"

Die Kommission hat – und dies ist positiv festzuhalten – nicht die Strategie des kleinsten gemeinsamen Nenners gewählt, der nur einige wenige, unumstrittene Grundsätze enthält und den Mitgliedsländern im übrigen freie Hand läßt. Dazu hätte es ausgereicht, die Europaratskonvention zu verbindlichem EG-Recht zu erklären. Die Kommission will vielmehr eine Harmonisierung auf dem von ihr so genannten „gleichwertigen nohen Schutzniveau", also eine Harmonisierung „nach oben" und nicht „nach unten" (Bundesrats-Drucks. 690/90, S. 16). Dies belegt auch die Tatsache, daß der Kommissionsvorschlag eine Reihe von Punkten enthält, die das Bundesdatenschutzgesetz in seiner derzeit noch geltenden Fassung nicht regelt; teilweise – aber keineswegs vollständig – finden sie sich im novellierten, am 1. Juni 1991 in Kraft tretenden BDSG (BGBl. 1990/I S. 2954) und in den neueren Landesdatenschutzgesetzen wie z.B. im Hessischen Datenschutzgesetz.

Dazu folgende Beispiele aus dem Text des Entwurfs: Die Richtlinie soll zwar nur für die Verarbeitung personenbezogener Daten in Dateien gelten (Art. 3). Sie wertet als Datei allerdings auch einen Text, aus dem mit Hilfe eines automatisierten Textverarbeitungsprogramms einzelne Daten feststellbar sind (Art. 2 lit c). Die „Verknüpfung" wird ausdrücklich als Phase der Datenverarbeitung genannt (Art. 2 lit d). Im nicht-öffentlichen Bereich wird bei der erstmaligen Datenweitergabe eine ausführliche Benachrichtigung des Betroffenen vorgeschrieben, so ist z.B. auch der Verarbeitungszweck mitzuteilen (Art. 9 Nr. 1). Vor Datenerhebungen beim Betroffenen ist u.a. über den Zweck zu unterrichten (Art. 13 Nr. 1 lit a). Die Zweckbindung erstreckt sich explizit auf die „Verwendung" der Daten; die Zweckfestlegung hat ausdrücklich zu erfolgen (Art. 16 Nr. 1 lit b). Entsprechend dem Vorbild im französischen Datenschutzgesetz wird das ausschließlich ADV-gestützte Persönlichkeitsprofil verboten (Art. 14 Nr. 2). Ein Automationsverbot mit wenigen, eng formulierten Ausnahmen gilt für besonders sensible Daten über Rasse, Religion, Gesundheit usw. (Art. 17 Nr. 1). Berichtigungen und Löschungen müssen den Datenempfängern mitgeteilt werden (Art. 14 Nr. 7).

Bei der Datensicherheit wird als eigenständige Maßnahme die Übertragungskontrolle bei der Benutzung öffentlicher Netze eingeführt (Art. 18 Nr. 2). Die Kommission will künftig selbst für die Datensicherheit verbindliche Standards vorgeben (Art. 18 Nr. 1). Vielleicht die Abweichung mit den größten praktischen Konsequenzen für speichernde Stellen im nicht-öffentlichen Bereich ist folgende Regelung: Den Vorbildern in Großbritannien und den Niederlanden entsprechend wird auch für sie die Meldepflicht zu einem von der Kontrollbehörde geführten Dateienregister statuiert (Art. 11).

2.5
Übermittlung ins Ausland

Besonderes Augenmerk richtet der Richtlinienvorschlag auf die Voraussetzungen für eine Datenübermittlung ins Ausland (Art. 24). Erfolgt diese in ein EG-Land, bleibt künftig kein Spielraum mehr für die Prüfung einer möglichen Verletzung „schutzwürdiger Belange" (vgl. z.B. § 24 BDSG), wenn dort die EG-Richtlinie in nationales Recht umgesetzt ist; der Einwand minderen oder fehlenden Datenschutzes im Empfängerland greift nicht mehr – das Essentiale des Entwurfs.

Anders bei Staaten außerhalb der EG. Datenexport dorthin ist grundsätzlich verboten, wenn dort kein – verglichen mit dem EG-Standard – „angemessenes Schutzniveau" besteht. Ausnahmen sind im Einzelfall möglich, wenn der Datenimporteur auf andere Weise, etwa durch die vertragliche Zusicherung von Schutzrechten, dieses Niveau sicherstellt (Art. 25). Allerdings ist dies nur nach vorheriger Unterrichtung der Kommission und ohne Widerspruch eines anderen Mitgliedstaates möglich. Auch hat das EG- „Exportland" die Pflicht, die Kommission zu informieren, wenn nach seiner Ansicht der Datenschutz im Zielland nicht ausreicht (Art. 24 Nr. 2). Die Kommission erhält die Befugnis, verbindlich die Angemessenheit des Schutzniveaus in Drittstaaten festzustellen (Art. 24 Nr. 4).

2.6
Weiteres Verfahren

Der Kommissionsvorschlag geht jetzt in das EG-Gesetzgebungsverfahren, u.a. muß er zweimal das Europäische Parlament passieren. Mit einer endgültigen Verabschiedung durch den Ministerrat kann wohl kaum vor 1992 gerechnet werden. Zahlreiche Einwände aus den nationalen Ministerialbürokratien und Wirtschaftsverbänden werden kommen, eine Situation, die ganz wesentlich durch den späten Zeitpunkt der Harmonisierung verursacht ist, der verantwortlich ist für die Auseinanderentwicklung der einzelstaatlichen Regelungsmodelle. Für das deutsche Datenschutzrecht sehe ich nach der erfolgten Novellierung des Bundesdatenschutzgesetzes kaum Anpassungsprobleme an die EG-Regelungen, immer unterstellt, sie werden im Gesetzgebungsverfahren durch die EG-Organe nicht allzusehr verändert. Am problematischsten ist wohl die Registermeldepflicht für Privatfirmen im Hinblick auf das Verhältnis von Aufwand und Nutzen einzustufen.

Die Datenschutzinstitutionen im Inland wie im Ausland haben sofort auf die Schritte der Kommission reagiert. Die 12. Internationale Konferenz der Datenschutzbeauftragten hat am 19. September 1990 in Paris beschlossen, noch im Verlauf des Jahres 1990 eine Sondersitzung von Vertretern der in den EG-Ländern bestehenden Kontrollorgane einzuberufen, um eine gemeinsame Position zu erarbeiten. Diese Tagung hat am 30. November 1990 in Wiesbaden stattgefunden. Die festgestellten Kritikpunkte und offenen Fragen sollen – voraussichtlich im Februar 1991 – mit der EG-Kommission in Brüssel besprochen werden. Nach der in Paris verabschiedeten Entschließung soll außerdem künftig jährlich ein Zusammentreffen der unabhängigen Beauftragten bzw. Kommissionen der Mitgliedstaaten stattfinden, um die EG-weite Abstimmung der jeweiligen Standpunkte zu verbessern.

Auch der unter meinem Vorsitz tagende „Arbeitskreis EG" der deutschen Konferenz der Datenschutzbeauftragten arbeitet an einer Stellungnahme zum Richtlinienvorschlag, die nach Verabschiedung durch die Konferenz Anfang 1991 den Regierungen in Bund und Ländern sowie den Entscheidungsgremien der EG zugeleitet werden soll.

Übereinstimmung besteht über die grundsätzlich positive Bewertung des Kommissionsentwurfs. Allerdings ist aus deutscher Sicht eine Reihe von Korrekturen notwendig. Dies gilt insbesondere für die Sicherstellung des Datenschutzes auf EG- Ebene. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten", die aus den Vertretern der nationalen Kontrollinstanzen besteht, muß unabhängig von der Kommission ihre Meinung bilden sowie zu allen datenschutzrelevanten Vorhaben ihre Stellungnahme abgeben können. Deshalb kann nicht – wie im Entwurf vorgesehen – ein Vertreter der EG-Kommission den Vorsitz dieses Gremiums führen, sondern nur ein von der Gruppe selbst gewähltes Mitglied. Die Pflicht der Kommission, alle Entwürfe mit Datenschutzbezug der Gruppe zur Begutachtung vorzulegen, muß unmißverständlich statuiert werden.

3. Personaldatenverarbeitung

3.1
Beihilfe für Angehörige eines Beamten

Einen unhaltbaren Zustand in der Praxis der Beihilfeabrechnung dokumentieren die beiden folgenden Fälle:

Ein Student, der sich in psychotherapeutischer Behandlung befindet, beschwerte sich bei mir darüber, daß ein Gutachten zur Beihilfefähigkeit seiner Behandlung zu der Beihilfeakte des allein beihilfeberechtigten Vaters genommen worden war. Der Vater hatte die Akte eingesehen und dabei den Inhalt des Gutachtens erfahren. Nach Darstellung des Studenten soll dadurch der Behandlungserfolg gefährdet worden sein.

In einem anderen Fall wandte sich eine in Scheidung lebende Frau dagegen, daß sie gezwungen sei, ihrem beihilfeberechtigten Ehemann ihre ärztlichen Befundunterlagen sowie die ihres gemeinsamen Kindes zugänglich zu machen, um eine Beihilfeunterstützung zu erhalten.

Nach den Vorschriften der Hessischen Beihilfenverordnung in der Fassung vom 11. Juli 1990 (GVBl. I S. 439) hat lediglich der Angehörige des öffentlichen Dienstes einen Anspruch auf Beihilfe. Nur er ist auch berechtigt, Beihilfe für Familienangehörige zu beantragen. Wollen diese eine Beihilfe in Anspruch nehmen, sind sie daher gezwungen, dem Beihilfeberechtigten die Belege, z.B. Arztrechnungen, Rezepte etc., aus denen sich in aller Regel die genauen Befunddaten ablesen lassen, zu geben.

Im ersten Fall war zwar das Gutachten der Festsetzungsstelle direkt übersandt worden, da der Beihilfeberechtigte aber das Recht hat, jederzeit die Beihilfeakte einzusehen, konnte der Vater ohne weiteres Kenntnis vom Inhalt des Gutachtens erlangen.

Ähnlich wie im Beihilferecht war in der Vergangenheit auch die Situation der Versicherten in der gesetzlichen Krankenversicherung. Durch das Gesundheitsreformgesetz vom 20.12.1988 (BGBl. I S. 2606) gelten jedoch die Familienangehörigen des Krankenkassenmitglieds nunmehr als Versicherte mit eigenem Antragsrecht.

Die bestehende Beihilferegelung ist mit dem Recht des einzelnen auf informationelle Selbstbestimmung nicht vereinbar. Daher habe ich das Hessische Innenministerium aufgefordert, nach dem Vorbild des Gesundheitsreformgesetzes die Hessische Beihilfenverordnung zu ändern und den Familienmitgliedern der Angehörigen des öffentlichen Dienstes einen selbständigen Anspruch gegenüber der Beihilfestelle zu gewähren.

Das Innenministerium lehnt eine solche Änderung jedoch ab, da es sich an einen Beschluß der Bund-Länder-Kommission für das Beihilferecht vom April 1989 gebunden sieht. Die Bund-Länder-Kommission vertritt in diesem Beschluß die Auffassung, daß die Beihilfe eine Ergänzung der Besoldung für bestimmte, nicht pauschal mit den Bezügen abgeltbare Teile des Lebensbedarfs darstelle. Der Anspruch auf Besoldung sei als höchstpersönliches Recht aber nicht teilbar, den Familienangehörigen stünde ein solcher Anspruch nicht zu. Ein eigener Beihilfeanspruch stehe somit im Widerspruch zu Art. 33 Abs. 5 Grundgesetz, der vorschreibt, daß das Recht des öffentlichen Dienstes unter Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums zu gestalten ist.

Dem ist entgegenzuhalten: Art. 33 Abs. 5 GG verlangt eine Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums. Dazu zählt z.B., daß das Beamtenverhältnis öffentlich-rechtlich auszugestalten ist und auf Lebenszeit eingegangen wird, nicht jedoch jede einzelne Regelung des früheren Beamtenrechts. Zu den Grundsätzen gehören nur die Prinzipien, die das Bild des Beamtentums in seiner überkommenen Form so prägen, daß ihre Beseitigung auch das Wesen des Beamtentums antasten würde. Das ist hier nicht der Fall.

Auch wenn man die derzeitige Ausgestaltung des Beihilfeanspruchs zu den hergebrachten Grundsätzen des Berufsbeamtentums zählen würde, ist eine Fortentwicklung keineswegs ausgeschlossen. Vielmehr entspricht es herrschender Rechtsauffassung, daß auch ein Abweichen von den hergebrachten Grundsätzen unter bestimmten Voraussetzungen zulässig ist.

Außerdem gibt Art. 33 Abs. 5 GG den hergebrachten Grundsätzen zwar Verfassungsrang, erhebt sie jedoch nicht über die übrigen Verfassungsbestimmungen. Die Regelung kann von anderen Verfassungsvorschriften eingeschränkt werden, wenn die Auslegung einen Vorrang einer anderen Verfassungsnorm ergibt. So sind beispielsweise frühere Bestimmungen des Beamtenrechts, wonach verheiratete Beamtinnen zwangsweise aus dem Dienst ausscheiden, verfassungswidrig und deshalb nicht mehr in Kraft. Im vorliegenden Fall hat das informationelle Selbstbestimmungsrecht der Angehörigen (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz) Vorrang.

3.2
Prüfung von Beihilfeanträgen durch das Rechnungsprüfungsamt

Eine Gemeinde bat mich um Stellungnahme zu der Frage, in welchem Umfang das Rechnungsprüfungsamt der Gemeinde eine begleitende Prüfung von Beihilfeanträgen vornehmen darf.

Beihilfedaten sind hochsensibel und unterliegen deshalb einem besonderen Schutz. Für Beihilfeangelegenheiten sind stets besondere Beiakten anzulegen, die getrennt von der Personalhauptakte geführt werden müssen und grundsätzlich nur den mit der Beihilfebearbeitung unmittelbar befaßten Stellen oder Bediensteten zugänglich sein dürfen.

Nach § 13 Abs. 4 Hessisches Datenschutzgesetz können jedoch auch Beihilfedaten für Aufsichtszwecke verwertet werden. Zur Grundvoraussetzung für eine funktionsfähige Rechnungsprüfung gehört zweifellos, daß der Prüfer eigenverantwortlich den Umfang seiner Prüfung festlegt; er ist insoweit nicht an Weisungen gebunden. Bei seiner Tätigkeit hat aber auch der Rechnungsprüfer das informationelle Selbstbestimmungsrecht des beihilfeberechtigten Beamten zu beachten. Das betrifft sowohl die Auswahl der Prüfungsfälle als auch den Umfang der Prüfung im Einzelfall.

Deshalb habe ich in Abstimmung mit dem Hessischen Innenministerium gegenüber den Kommunalen Spitzenverbänden die folgende Verfahrensweise angeregt, die einen angemessenen Interessenausgleichs zwischen dem gesetzlichen Auftrag der Rechnungsprüfer und dem informationellen Selbstbestimmungsrecht der Beihilfeantragsteller sicherstellt.

Soweit der Rechnungsprüfer Beihilfebescheide vor der Auszahlung prüft, erhält er zunächst nur die Aufstellung über die einzelnen Leistungen mit der errechneten Leistungssumme. Die Arztrechnungen (inkl. der Diagnosen) und Rezepte werden in einem verschlossenen Umschlag mitgereicht. Nur wenn der Rechnungsprüfer Zweifel an der Plausibilität der Abrechnung hat, öffnet er den Umschlag und überprüft die Richtigkeit der Aufstellung anhand der Belege.

Damit wird die Kenntnisnahme von Diagnosen usw. auf Einzelfälle beschränkt, in denen dies zur Überprüfung erforderlich ist. Das zwingt den Prüfer, sich jeweils darüber klar zu werden, ob Einsicht in die Belege erfolgen muß und dient damit dem Interesse des Beihilfeantragstellers, den Kreis der Personen, die seine Krankheitsdaten erfahren, so klein wie möglich zu halten. Der Hessische Landkreistag hat mir inzwischen mitgeteilt, daß er seine Mitglieder um Beachtung dieser Grundsätze gebeten hat.

3.3
Novellierung der Hessischen Beihilfenverordnung und der Verwaltungsvorschrift zur Durchführung der Beihilfenverordnung

Am 1. August ist die novellierte Hessische Beihilfenverordnung und am 1. Oktober die dazu ergangene Verwaltungsvorschrift in Kraft getreten (GVBl. I S. 439 bzw. StAnz. 1990 S. 1604). Leider sind meine Änderungsvorschläge, die ich dem Hessischen Innenministerium zum Entwurf der Verwaltungsvorschrift unterbreitet hatte, weitgehend unberücksichtigt geblieben.

Zu kritisieren sind hauptsächlich die Regelungen zur Einholung von Gutachten bzw. Obergutachten über die Beihilfefähigkeit psychotherapeutischer Behandlungen. Schon in meiner Stellungnahme zu der am 5. Mai 1988 vorgenommenen Änderung der Verwaltungsvorschriften zur Hessischen Beihilfenverordnung hatte ich mich vergeblich dagegen gewandt, daß die Einzelheiten des Bewilligungsverfahrens für Psychotherapien lediglich in den Verwaltungsvorschriften zur Beihilfenverordnung und nicht in der Verordnung selbst geregelt sind. Sein informationelles Selbstbestimmungsrecht kann der Bürger nur ausüben, wenn die Datenflüsse transparent sind. Das ist jedoch nicht der Fall, wenn Regelungen nur in für den Bürger schwer zugänglichen Verwaltungsvorschriften getroffen werden.

Meiner Forderung nach Anonymisierung des Arztberichts, der im Rahmen des Bewilligungsverfahrens für psychotherapeutische Behandlungen dem von der Festsetzungsstelle benannten Gutachter zugesandt wird, wurde ebenfalls nicht entsprochen. Dem Gutachter werden weiterhin Name, Vorname, Geburtsdatum, Geschlecht und Beruf mitgeteilt. Darüber hinaus sieht die Neuregelung vor, daß die Festsetzungsstelle einen weiteren, sog. Obergutachter benennen kann, der seinerseits den Bericht des behandelnden Arztes mit den genauen Angaben zur Diagnose und Prognose und dem vollständigen Namen des Patienten erhält. Der Kreis von Personen, der somit über intimste Daten des Patienten Kenntnis erlangt, wird dadurch noch erweitert. Dabei ist die Kenntnis des Namens des Patienten für die Begutachtung durch den Erst- oder Obergutachter überhaupt nicht erforderlich, da der Gutachter mit dem betroffenen Patienten keinen Kontakt aufnimmt und keine persönliche Untersuchung vornimmt. Deshalb werden z.B. im Bereich der gesetzlichen Krankenkassen die ärztlichen Unterlagen an den Gutachter ohne Namensnennung unter einer Chiffrenummer weitergeleitet.

Der Hessische Innenminister hat in der Vergangenheit darauf verwiesen, daß die Gutachter der ärztlichen Schweigepflicht unterliegen und deshalb eine Anonymisierung nicht erforderlich sei. Dem steht jedoch das Hessische Datenschutzgesetz entgegen. Danach dürfen auch an Personen, die besondere Geheimhaltungsvorschriften einzuhalten haben, personenbezogene Daten nur in dem zur Aufgabenerfüllung erforderlichen Umfang weitergegeben werden.

Die Übermittlung an den Gutachter wird auch nicht durch die in der Verwaltungsvorschrift vorgesehene Einwilligungserklärung des Patienten in die Offenbarung seiner Gesundheitsdaten zulässig. In meiner Stellungnahme zum Entwurf hatte ich deutlich gemacht, daß eine pauschale Entbindung des Arztes von der Schweigepflicht unwirksam ist und daher nicht zur Übersendung der personenbezogenen Krankenunterlagen an Gutachter und Obergutachter berechtigt, denn der Patient muß im einzelnen nachvollziehen können, an welche Personen seine Krankheitsdaten übermittelt werden. In der jetzt gültigen Fassung der Verwaltungsvorschrift ist die Einwilligungserklärung daher um folgenden Zusatz ergänzt worden:

„Die Schweigepflichtentbindung gilt auch, wenn ein Obergutachter mit der Erstellung eines Gutachtens beauftragt wird."

Ich halte auch diese Einwilligungserklärung für unzureichend. Sie läßt für den Patienten und Beihilfeantragsteller nicht erkennen, ob tatsächlich ein Obergutachter benannt wird. Noch schwerer wiegt, daß jegliche Information darüber fehlt, an wen die Krankenunterlagen weitergeleitet werden. Bei derartig sensiblen Daten muß der Patient wissen, wer Kenntnis von seinen Daten erhält. Vor allem muß er die Möglichkeit haben, im Einzelfall die Weitergabe an einen bestimmten Arzt zu verweigern. Von der wirksamen Einwilligung kann daher nur gesprochen werden, wenn für den Betroffenen erkennbar ist, an wen die Daten übermittelt werden.

Eine kleine Verbesserung hat dagegen das Beihilfeantragsformular erfahren. Das Geburtsdatum und die Arbeitsstelle des Ehegatten müssen künftig nicht mehr angegeben werden.

4. Sozialverwaltung

4.1
Köpenickiade im Kreisjugendamt

Der Fall „Peter Graf", der schon seit längerem für Schlagzeilen in der Presse sorgt, hat im vergangenen Jahr auch den Hessischen Datenschutzbeauftragten beschäftigt.

Die Mutter eines nichtehelichen Kindes stand im Verdacht, zusammen mit einem Boxveranstalter den Vater der Tennisspielerin Steffi Graf mit der Behauptung, er sei der Vater ihres Kindes, erpreßt zu haben. In der Presse war auch darüber berichtet worden, daß die Staatsanwaltschaft gegen die Mutter und den Boxveranstalter ermittelte. Beim Kreisjugendamt in Bad Schwalbach, das die Amtsvormundschaft über das Kind führt, rief eines Tages ein Mann an, der sich als Staatsanwalt ausgab und erklärte, die Staatsanwaltschaft ermittele wegen Falschaussage gegen die Mutter des Kindes. Wenn das Jugendamt Unterlagen über die Amtspflegschaft führe, wolle man diese einsehen. Als der Anrufer später im Jugendamt erschien, wurden ihm, ohne seine Identität zu überprüfen, die Akten vorgelegt. Kurze Zeit später veröffentlichte die Illustrierte „Quick" Ablichtungen von Schreiben des Jugendamtes, die in den Akten enthalten waren. Das Jugendamt war einem Journalisten auf den Leim gegangen.

Diese Köpenickiade war nur möglich, weil die Mitarbeiter des Jugendamtes völlig unzureichend mit dem Sozialdatenschutz vertraut waren.

Die Vormundschaftsdaten des Jugendamtes sind Sozialdaten, die dem Sozialgeheimnis nach § 35 Abs. 1 Sozialgesetzbuch I (SGB I) unterliegen. Das Sozialgesetzbuch X (SGB X) regelt in § 73 detailliert, unter welchen Voraussetzungen diese Daten Strafverfolgungsbehörden bekanntgegeben werden dürfen: Ohne richterliche Anordnung ist die Mitteilung von Sozialdaten an Strafverfolgungsbehörden unzulässig. Wird wegen eines Vergehens ermittelt, beschränkt sich die Offenbarungsbefugnis auf Angaben über Vor- und Familiennamen, Geburtsdatum und -ort sowie derzeitige und frühere Anschriften des Betroffenen bzw. seines Arbeitgebers sowie Angaben über erbrachte Geldleistungen. Bei Ermittlungen wegen eines Verbrechens können alle erforderlichen Daten übermittelt werden. Der Richter hat bei einer Entscheidung, ob und in welchem Umfang er die Offenbarung von Sozialdaten anordnet, auch den Verhältnismäßigkeitsgrundsatz zu beachten. Er muß jeweils genau die Daten bestimmen, die offenbart werden dürfen. Dabei spielt die Schwere der Straftat eine entscheidende Rolle.

Übermittelt werden dürfen nur Daten derjenigen Person, gegen die als Täter ermittelt wird. § 73 SGB X gibt weder eine Möglichkeit zum Datenabgleich im Sinne einer Rasterfahndung noch eine Befugnis zum Übermitteln von Daten von Personen, die als Zeugen in einem Ermittlungsverfahren beteiligt sind.

Das Jugendamt verstieß somit gleich mehrfach gegen das Datenschutzrecht. Weder lag eine richterliche Anordnung vor, noch war das Kind Betroffener im Ermittlungsverfahren. Zudem wäre selbst bei richterlicher Anordnung eine unbeschränkte Akteneinsicht nicht in Betracht gekommen, denn eine uneidliche Falschaussage ist kein Verbrechen, sondern ein Vergehen. Besonders leichtfertig war schließlich, die Akte jemandem vorzulegen ohne dessen Identität und Berechtigung zu überprüfen und ohne sich Gedanken darüber zu machen, ob und wenn ja welche Informationen überhaupt offenbart werden durften.

Auf meine förmliche Beanstandung habe ich eine äußerst erstaunliche Stellungnahme des Kreisausschusses erhalten. Darin heißt es, das Jugendamt habe im besten Glauben der Staatsanwaltschaft bei der Aufklärung eines Verbrechens helfen wollen. Der langjährige fachkundige Sachbearbeiter habe nicht wissen können, daß ohne richterliche Anordnung auf keinen Fall eine Akteneinsicht hätte erfolgen dürfen.

4.2
Beschlagnahme von Jugendamtsakten

Einem Jugendamt wurde in einem anonymen Brief eine Kindesmißhandlung angezeigt. Die Ermittlungen des Jugendamtes ergaben, daß die Anschuldigungen unzutreffend waren. Daraufhin erstatteten die beschuldigten Eltern Strafanzeige. Im Rahmen des Ermittlungsverfahrens verlangte die Staatsanwaltschaft die Vorlage des Briefes. Das Jugendamt hatte jedoch Zweifel an der Rechtmäßigkeit des Verlangens der Staatsanwaltschaft und bat mich deshalb um Stellungnahme.

Das Jugendamt durfte den Brief unter den gegebenen Umständen nicht der Staatsanwaltschaft vorlegen. Zwar können Sozialbehörden für die Durchführung eines mit ihrer Aufgabenerfüllung zusammenhängenden Strafverfahrens Sozialdaten Dritten offenbaren, wenn dies erforderlich ist (§ 69 Abs. 1 Nr. 1 Sozialgesetzbuch X). Das Jugendamt sah im vorliegenden Fall dazu jedoch keine Notwendigkeit. Auch die Voraussetzungen für eine richterliche Anordnung der Vorlage des Briefes waren nicht erfüllt. Gemäß § 73 Sozialgesetzbuch (SGB) X kann der Richter die Offenbarung von Sozialdaten anordnen, soweit dies zur Aufklärung eines Verbrechens, also einer mit mindestens ein Jahr Freiheitsstrafe bedrohten Straftat, erforderlich ist. Zur Aufklärung eines Vergehens ist nur die Offenbarung von Angaben über Vor- und Familiennamen, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen sowie Namen und Anschriften seiner derzeitigen und früheren Arbeitgeber und Angaben über erbrachte oder demnächst zu erbringende Geldleistungen zulässig. Da es im vorliegenden Fall nicht um einen besonders schweren Fall von Kindesmißhandlung, d.h. um ein Verbrechen (§ 223b Abs. 2 Strafgesetzbuch) ging,

sondern um die einfache Mißhandlung eines Schutzbefohlenen (§ 223b Abs. 1 StGB), also um ein Vergehen, hätten der Staatsanwaltschaft nur die aufgezählten Angaben mitgeteilt werden dürfen. Die für die Strafverfolgung notwendigen Angaben wie Name und Anschrift ergaben sich jedoch gerade nicht aus der anonymen Anzeige. Das Jugendamt hat deshalb auf meinen Rat die Herausgabe des Schreibens zunächst verweigert.

Später mußte das Amt dann allerdings doch der Staatsanwaltschaft den Brief übergeben. Ein Richter hatte gem. § 73 SGB X die Herausgabe angeordnet. Um die Auseinandersetzung mit den Eltern und der Staatsanwaltschaft zu beenden, hatte der Dezernent auf eine Beschwerde gegen die Entscheidung verzichtet.

4.3
Unnötig detaillierte Erziehungsberichte

Einer der sensibelsten Bestandteile der Akten, die die Jugendämter über einzelne Jugendliche führen, sind die Erziehungsberichte. Das Jugendamt erhält diese Berichte in seiner Eigenschaft als Kostenträger von den Heimen, in denen die Jugendlichen untergebracht sind. Die Erziehungsberichte dienen als Grundlage für die Entscheidung über die weitere Gewährung von Leistungen der Jugendhilfe. Das Jugendamt benötigt jedoch für seine Entscheidung, ob gerade die gegenwärtige Hilfe die richtige ist und/oder ob zusätzliche Maßnahmen erforderlich sind, keine derartig ausführlichen Berichte, wie sie derzeit von den Betreuern und Therapeuten geliefert werden. Die Angaben müssen erheblich reduziert werden. Davon konnte ich mittlerweile auch die Jugendämter und die Mitarbeiter der Heime überzeugen.

Eine Reduzierung des Inhalts der Erziehungsberichte hat außerdem einen für die Jugendämter vorteilhaften Nebeneffekt: Die Konflikte mit den Eltern, die die Akten über ihre Kinder einsehen wollen, werden stark zurückgehen. Die Berichte werden z.Z. oft als vertraulich gekennzeichnet. Damit soll ein angemessener Umgang mit diesen Unterlagen innerhalb des Jugendamtes sichergestellt werden. Manche Berichte tragen darüber hinaus noch den Aufdruck: „Nicht für die Hand von Eltern und Jugendlichen." Grund hierfür ist die Sorge, der Therapieerfolg und die weitere Entwicklung der Kinder könne gefährdet werden, wenn die Eltern die ausführlichen Berichte über die Entwicklung und Bewertung ihrer Kinder lesen würden. Das Akteneinsichtsrecht, das § 25 SGB X den Eltern gewährt, kann zwar eingeschränkt werden, wenn das berechtigte Interesse eines anderen Verfahrensbeteiligten es erfordert. Das Kind ist im Verhältnis zu seinen Eltern jedoch kein anderer Verfahrensbeteiligter. Die Eltern nehmen vielmehr als gesetzliche Vertreter ihrer Kinder deren Rechte als Verfahrensbeteiligte wahr. Ihnen gegenüber gibt es daher keine Möglichkeit zur Beschränkung der Akteneinsicht. Die Sorge des Jugendamtes erledigt sich allerdings, wenn der Inhalt der Erziehungsberichte auf das für die Aufgabenerfüllung erforderliche Maß reduziert wird.

5. Gesundheit

5.1
Prüfungen der klinischen Krebsregister in den Städtischen Kliniken Darmstadt und Kassel sowie dem Universitätsklinikum Gießen

5.1.1
Funktion der klinischen Krebsregister

Klinische Krebsregister werden seit einigen Jahren in den Tumorzentren bzw. den onkologischen Schwerpunktkrankenhäusern (z.Z. Frankfurt, Gießen, Darmstadt, Kassel, Fulda und Limburg) aufgebaut. Sie dienen der Verbesserung der Behandlung – einschließlich der Nachsorge – der darin erfaßten Patienten, indem die wesentlichen bei der Behandlung anfallenden Daten automatisiert gespeichert und im Interesse einer interdisziplinären Zusammenarbeit den verschiedenen (mit-) behandelnden Ärzten eines Patienten als vollständige Informationsbasis für die Behandlung zugänglich gemacht sowie zur Qualitätskontrolle der Behandlung statistisch aufbereitet werden. Darüber hinaus sollen diese Register auch Arzt und Patienten bei der Einhaltung von Kontroll- und Nachsorgeterminen unterstützen.

Die klinischen Krebsregister sind damit strikt zu unterscheiden von epidemiologischen, d.h. bevölkerungsbezogenen Krebsregistern, die nicht in einem unmittelbaren Zusammenhang mit der Behandlung der gespeicherten erkrankten Personen stehen. In epidemiologischen Registern werden alle Neuerkrankungen einer bestimmten Region (z.B. eines Bundeslandes) gespeichert. Durch die kontinuierliche Beobachtung der Häufigkeit aller Formen von Krebserkrankungen in der gesamten Bevölkerung dieser Region erhofft man sich, Änderungen der Erkrankungshäufigkeit zu erkennen, die auf mögliche neu entstandene Krebsgefährdungen hinweisen, und die Häufigkeit und Verteilung innerhalb der Regionen feststellen sowie auf umweltbezogene und individuelle Krebsrisiken untersuchen zu können. Ein epidemiologisches Krebsregister gibt es in Hessen derzeit nicht. In einigen anderen Bundesländern ist ein solches Register vorhanden. Es bedarf in jedem Fall einer gesetzlichen Grundlage (s. hierzu auch den Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 04./05. Oktober 1990, Ziff. 17.3.7 dieses Berichts).

5.1.2
Datenschutz-Gesamtkonzept für die klinischen Krebsregister

5.1.2.1
Rechtliche Anforderungen

Aufgrund von Prüfungserfahrungen hatte ich im Jahre 1986 ein einheitliches Datenschutz-Gesamtkonzept für alle klinischen Krebsregister in Hessen gefordert. Seit 1989 gibt es nunmehr ein solches Gesamtkonzept (siehe 15. Tätigkeitsbericht, Ziff. 4.2; 17. Tätigkeitsbericht, Ziff. 5.3; 18. Tätigkeitsbericht, Ziff. 18.3). Deshalb habe ich mich 1990 eingehend über den Stand des Aufbaus der Register und der Umsetzung des Datenschutz-Gesamtkonzepts in verschiedenen Kliniken informiert.

Der Hauptgrund für die Entwicklung des Datenschutz-Gesamtkonzepts war, daß in den klinischen Krebsregistern der onkologischen Schwerpunktkrankenhäuser die Daten von Patienten verschiedener Fachabteilungen bzw. Institute innerhalb des onkologischen Schwerpunktkrankenhauses, darüber hinaus die Daten von Patienten anderer Krankenhäuser und auch niedergelassener Ärzte zusammengeführt werden. Auf eine gesetzliche Grundlage für ein solches Register kann nur dann verzichtet werden, wenn besondere Vorkehrungen getroffen werden, die das informationelle Selbstbestimmungsrecht der betroffenen Patienten hinreichend und dauerhaft sichern. Es muß gewährleistet sein, daß der Zusammenhang zwischen der Behandlung der Patienten und der Verarbeitung ihrer personenbezogenen Daten im Register bestehen bleibt. Die rechtliche Verantwortlichkeit der jeweiligen speichernden Stelle bzw. der jeweiligen behandelnden Ärzte für die Daten ihrer Patienten muß gewahrt bleiben. Zentrale Forderungen des Datenschutz-Gesamtkonzepts sind daher insbesondere die folgenden Punkte:

- Im Register des onkologischen Schwerpunktkrankenhauses dürfen die Daten von Patienten niedergelassener Ärzte oder von anderen Krankenhäusern nur erfaßt werden, wenn eine Einwilligung der Patienten vorliegt, denn es besteht kein Behandlungsvertrag zwischen dem onkologischen Schwerpunktkrankenhaus und dem Patienten, sondern zwischen dem niedergelassenen Arzt bzw. dem anderen Krankenhaus und dem Patienten. Das onkologische Schwerpunktkrankenhaus verarbeitet die Daten dieser Patienten im Auftrag der niedergelassenen Ärzte bzw. der anderen Krankenhäuser (§ 4 Hessisches Datenschutzgesetz). Die Weitergabe der Patientendaten an das onkologische Schwerpunktkrankenhaus ist eine Durchbrechung der ärztlichen Schweigepflicht im Sinne von § 203 Strafgesetzbuch.

- Für die Datenverarbeitung im Auftrag ist in jedem Fall ein schriftlicher Vertrag erforderlich, der festlegt, welche Daten zu welchem Zweck in dem Register verarbeitet werden, insbesondere wer in welchem Verfahren die personenbezogenen Daten der betroffenen Patienten erhält. Für die niedergelassenen Ärzte hat die Kassenärztliche Vereinigung in Abstimmung mit mir ein entsprechendes Vertragsformular entwickelt.

- Die online-Zugriffsmöglichkeiten innerhalb des onkologischen Schwerpunktkrankenhauses müssen auf die jeweiligen den Patienten (mit-) behandelnden Fachabteilungen beschränkt sein. Das Krankenhaus ist keine informationelle Einheit, in der personenbezogene Daten beliebig ausgetauscht werden dürfen. Die ärztliche Schweigepflicht und § 12 Abs. 2 und 3 des Hessischen Krankenhausgesetzes gebieten eine Abschottung der Datenbestände der einzelnen Fachabteilungen untereinander. Grundsätzlich sind auch für die Aufgabenerfüllung einer Fachabteilung die Datenbestände einer anderen Fachabteilung nicht erforderlich. Eine Fachabteilung darf nur dann Zugriff auf die personenbezogenen Daten eines Patienten einer anderen Fachabteilung haben, wenn sie diesen Patienten mitbehandelt. Erst recht darf es selbstverständlich keinen generellen online-Zugriff eines anderen Krankenhauses auf die Registerdaten geben, sondern das andere Krankenhaus darf nur Zugriff auf die Daten derjenigen Patienten haben, die es selbst (mit-) behandelt.

- Das Verfahren der Erstellung und Weitergabe von Auswertungen aus dem Register muß klar und kontrollierbar ausgestaltet sein.

- Personenbezogene Auswertungen dürfen nur die jeweiligen (mit-) behandelnden Ärzte der betreffenden Patienten erhalten.

  Die Anforderungen von personenbezogenen Auswertungen aus dem Register durch die Ärzte müssen formularmäßig dokumentiert werden. Aus dem Formular muß eindeutig und vollständig ersichtlich sein, welche konkreten Auswertungen der Arzt angefordert hat und es muß die Unterschrift des Arztes enthalten. Zusätzlich zu dieser Dokumentation muß eine automatisierte Protokollierung der im Register durchgeführten Auswertungen erfolgen, mittels deren festgestellt werden kann, welche Auswertungen tatsächlich erstellt wurden.

- Damit der Zusammenhang zwischen der Verarbeitung der Daten im Register und der Behandlung der Patienten gewahrt bleibt, müssen Vorkehrungen getroffen sein, daß der Personenbezug der im Register gespeicherten Daten spätestens 15 Jahre nach Behandlungsabschluß beseitigt wird.

5.1.2.2
Räumliche, technische und organisatorische Anforderungen

Die besondere Sensibilität und der Umfang des Datenbestandes erfordern entsprechende technische, organisatorische und räumliche Sicherungsmaßnahmen in den onkologischen Schwerpunktkrankenhäusern. Insbesondere geht es dabei darum, daß die einzelnen Maßnahmen sich zu einem Gesamtsystem ergänzen.

- Die Räume der klinischen Krebsregister dürfen nur von befugten Personen betreten werden können. Da nicht jeder Mitarbeiter der Krebsregister alle Räume betreten muß, sind die Räumlichkeiten in 3 Sicherheitsbereiche SB1, SB2 und SB3 zu unterteilen, zu denen differenzierte Zugangsberechtigungen vorzusehen sind. Dabei umfaßt der SB1 die Räume, in denen der Rechner installiert ist und gegebenenfalls die Auswertungen, Ausdrucke, Sicherungen usw. vorgenommen werden. Zum SB2 gehören die Räume, in denen die Dokumentation, die Datenerfassung und die DV- Entwicklung vorgenommen werden. Der SB3 besteht aus den anderen Räumen, in denen mit den personenbezogenen Daten des Tumorregisters gearbeitet wird. Die besonders sensiblen Sicherheitsbereiche SB1 und SB2 müssen in dem Schließsystem des Krankenhauses einen eigenen Bereich haben. Die Vergabe der Schlüssel muß restriktiv erfolgen und dokumentiert sein. Ferner sind die Mitarbeiter namentlich zu benennen, die Zutritt zu diesen Sicherheitsbereichen haben. Betreten andere Personen diese Bereiche, so darf dies nur unter Aufsicht eines Zutrittsberechtigten erfolgen und es muß dies in einem Besucherbuch protokolliert werden. Die Räume sind verschlossen zu halten, was auch für den SB3 gilt.

Die DV-technischen Sicherungsmaßnahmen müssen dem Stand der Technik von Fall zu Fall angeglichen werden. Daher sind die im Datenschutz-Gesamtkonzept genannten Maßnahmen mehr als Richtschnur aufzufassen. Besonders wichtig sind die folgenden technischen und organisatorischen Maßnahmen:

- Die Anmeldung am System muß die Eingabe einer Benutzerkennung und eines Passwortes verlangen. Nur wenn das Passwort richtig eingegeben wurde, hat sich der Benutzer gegenüber dem DV-System ausgewiesen und darf die Möglichkeiten haben, mit dem DV-System zu arbeiten. Damit bei der Kontrolle von Datenzugriffen und bei Protokollierungen auch feststeht, welche Person gerade tätig war, muß eine Benutzerkennung genau einer Person zugeordnet sein. (Zur Passwortverwaltung vgl. Ziff. 15.5).

- Für jeden Benutzer ist ein Profil zu erstellen, das die Berechtigungen auf dem DV-System festlegt. Diese Berechtigungen müssen dann automatisch bei der Benutzung des Systems kontrolliert werden. Dies ist nur möglich, wenn wie gefordert, jede Benutzerkennung genau einer Person zugeordnet ist.

- Die Benutzer dürfen die ihnen zugewiesenen Anwendungsfunktionen nicht verlassen können. Insbesondere darf nur der Systemverantwortliche auf die Systemebene gelangen können. Anderenfalls stehen dem normalen Benutzer Systemfunktionen zur Verfügung, die er nicht benötigt und die auch die Möglichkeiten bieten, weitergehende Berechtigungen zu erlangen.

- Die Inanspruchnahme von Anwendungsfunktionen muß automatisch protokolliert werden. Zusammen mit der Dokumentation der Berechtigungsprofile ist es möglich festzustellen, welcher Benutzer wann auf welche Daten zugegriffen hat. Die Dokumentation der Berechtigungsprofile muß die auf dem DV-System geltenden Zugriffsrechte wiedergeben. Dies kann nur erreicht werden, wenn automatisierte Auswertungen die entsprechenden Systemdateien auswerten.

- Es muß die ordnungsgemäße Datenverarbeitung sichergestellt werden. Dazu gehört unter anderem die Durchführung von Abschlußtests, die schriftliche Freigabe der Programme, die Verfahrensdokumentation und nicht zuletzt die Funktionstrennung zwischen Programmierung und Produktion, also der Betreuung der Anwendung und des Rechners.

- Die Vernichtung von Datenträgern (Magnetbänder, Disketten, Carbonbänder, Auswertungen, Ausdrucke usw.) muß auch unabhängig von den Forderungen des Datenschutz-Gesamtkonzeptes geregelt sein (vgl. Ziff. 15.3).

Alle aufgeführten Punkte müssen in einer Dienstanweisung festgelegt sein.

5.1.3
Prüfungsergebnisse

Bei meinen 1990 durchgeführten Prüfungen lag der Schwerpunkt bei den Kliniken, die bereits Daten externer Patienten im Register verarbeiten. Dies sind die Städtischen Kliniken Darmstadt, in deren Register zum Zeitpunkt der Prüfung Daten von etwa 8.000 Patienten gespeichert waren, davon etwa 2.400 externe Patienten, und die Städtischen Kliniken Kassel, in deren Register zum Zeitpunkt der Prüfung Daten von etwa 4.000 eigenen Patienten und von 128 Patienten niedergelassener Ärzte gespeichert waren. Darüber hinaus habe ich das Krebsregister des Universitätsklinikums Gießen geprüft, das zum Zeitpunkt der Prüfung Daten von etwa 10.000 eigenen Patienten enthielt. Voraussichtlich wird 1991/92 mit der Speicherung der Daten externer Patienten begonnen.

5.1.3.1
Rechtliche Mängel

In allen drei Kliniken werden in den Registern nur solche Daten erfaßt, die im Zusammenhang mit der Behandlung des Patienten erhoben wurden. Der Behandlungszusammenhang ist insoweit gewahrt. Folgende Mängel waren jedoch festzustellen:

- Es lagen nicht in allen Fällen Verträge über die Auftragsdatenverarbeitung vor. In den Städtischen Kliniken Kassel waren zwar bereits Patientendaten niedergelassener Ärzte erfaßt, es existierten jedoch keine schriftlichen Verträge zwischen den niedergelassenen Ärzten und den Städtischen Kliniken über die von den Städtischen Kliniken durchzuführende Datenverarbeitung im Auftrag vor. In Darmstadt lagen diese Verträge vor, die Patientendaten der niedergelassenen Ärzte wurden nur dann ins Register aufgenommen, wenn ein schriftlicher Vertrag vorlag. Auch für die im Auftrag der Ärzte des Elisabethenstifts vorgenommene Datenverarbeitung lagen schriftliche Verträge vor. Der Vertragstext war allerdings fehlerhaft.

- In allen drei Kliniken waren die Möglichkeiten des online-Zugriffs zu weitgehend. Innerhalb der Städtischen Kliniken Darmstadt hatte die Abteilung Strahlentherapie nicht nur auf die Daten derjenigen Patienten Zugriff, die von dieser Abteilung (mit-)behandelt wurden, sondern Zugriff auf die Stammdaten (d.h. Name, Geburtsdatum, Adresse, Nationalität, Beruf, einweisender Arzt/Hausarzt/Mitbehandelnde) aller im Register erfaßten Patienten der Städtischen Kliniken. Diese Zugriffsmöglichkeiten wurden nach meiner Prüfung abgestellt. Darüber hinaus hatte das Elisabethenstift die Möglichkeit des Zugriffs auf alle im Krebsregister gespeicherten Stammdaten der Patienten der Städtischen Kliniken. Noch während meiner Prüfung wurde die Datenleitung des Elisabethenstifts mechanisch vom Rechner der EDV-Abteilung getrennt und die Kennworte für die dortigen Mitarbeiterinnen auf dem Rechner gelöscht. Das Elisabethenstift darf künftig nur auf seine eigenen Patientendaten zugreifen.

  Innerhalb der Städtischen Kliniken Kassel hatten die Hautklinik und die Klinik für Urologie die Möglichkeit, auf alle im Register gespeicherten Stammdaten der Patienten der Städtischen Kliniken zuzugreifen.

  Innerhalb des Universitätsklinikums Gießen konnte jede am Register beteiligte Fachabteilung bzw. jedes Institut auf alle Patientenstammdaten und darüber hinaus sogar noch auf die Tumorbasisdaten aller im Register gespeicherten Patienten zugreifen.

  Die Kliniken haben mir zugestimmt, daß diese Zugriffsmöglichkeiten der einzelnen Fachabteilungen für die Behandlung der Patienten nicht erforderlich sind. Die bisherige Verfahrensweise wurde damit begründet, daß der Zugriff auf den Gesamtbestand der Patientenstammdaten nötig sei, um eine Doppelerfassung von Patienten, die gleichzeitig in verschiedenen Fachabteilungen behandelt werden, zu vermeiden. Hierzu wird vor der Erfassung neuer Patientendaten auf Wunsch eine Liste aller gespeicherten Patientenstammdaten zum Abgleich angezeigt. Das sind sogar noch wesentlich mehr Daten als zur Vermeidung von Doppelerfassungen benötigt würden. Ich habe die Kliniken auf programmtechnische Maßnahmen hingewiesen, die eine Doppelerfassung ausschließen, ohne daß Patientendaten unzulässig offenbart werden. So könnte z.B. bei der Ersterfassung vor dem ersten Abspeichern eines Patientenstammsatzes automatisch geprüft werden, ob ein Stammsatz mit identischen Namen und Geburtsdaten gespeichert ist. Abhängig vom Ergebnis dieser Prüfung kann der Erfassungsdatensatz entweder gespeichert oder bei Übereinstimmung der schon vorhandene Stammdatensatz angezeigt werden.

- Das Verfahren der Erstellung und Weitergabe von Auswertungen bedarf in allen drei Kliniken der Verbesserung. In jeder der drei Kliniken erhalten nur die jeweils behandelnden Fachabteilungen für ihre eigenen Patienten personenbezogene Auswertungen aus dem Register. Damit ist in diesem Punkt die Abschottung der Datenbestände der Fachabteilungen untereinander entsprechend der Rechtslage und dem Datenschutz-Gesamtkonzept umgesetzt. In den Städtischen Kliniken Darmstadt und Kassel ist das Formular zur Anforderung von Auswertungen zu ändern. Außerdem muß in Darmstadt sichergestellt werden, daß auf dem Formular in jedem Fall die Unterschrift des anfordernden Arztes enthalten ist. In Darmstadt und Gießen wurde keine automatisierte Protokollierung der durchgeführten Auswertungen vorgenommen.

- Vorkehrungen, die eine Löschung des Personenbezugs der im Krebsregister gespeicherten Daten spätestens 15 Jahre nach Abschluß der Behandlung sicherstellen, müssen noch in allen drei Kliniken getroffen werden.

- In allen drei Kliniken bedürfen die Dienstanweisungen noch der Vervollständigung bzw. der Umarbeitung.

5.1.3.2
Datensicherheitsmängel

5.1.3.2.1
Technische und organisatorische Mängel

Bei der Prüfung der technischen Ausgestaltung des Datenschutzes mußte ich große durch veraltete Betriebssystem-Software hervorgerufene Probleme feststellen. Diese Software, die die Verbindung zwischen der Anwendung „Tumorregister" und dem Rechner herstellt, wurde vor einigen Jahren ausgewählt. Seitdem sind die Datensiche-

rungsfunktionen der eingesetzten Betriebssysteme nicht in ausreichendem Maße weiterentwickelt worden. Im Vergleich zu anderen Betriebssystemen ergeben sich Defizite im Bereich der Benutzerkontrolle und der Protokollierung. Diese Mängel konnten bislang durch die Kliniken nur mit großem Aufwand und trotzdem nicht immer voll befriedigend ausgeräumt werden. Es muß daher im Einzelfall geprüft werden, wie die weitere Entwicklung in einem DV-Gesamtsystem für die Kliniken aussehen kann. Dabei ist auch die zukünftige Entwicklung auf dem Gebiet der Betriebssystem- und Datenbanksoftware durch die Entscheidungsgremien zu berücksichtigen. Im einzelnen zeigten sich folgende Mängel:

- Da mit der eingesetzten Datenbanksoftware und dem Betriebssystem eine Umsetzung der Forderungen des Datenschutz-Gesamtkonzeptes nicht möglich war, entschied sich die Universitätsklinik Gießen für eine komplette Neuentwicklung des Verfahrens. Dabei wird ein UNIX-Rechner mit einer relationalen Datenbank verwendet. Das neue System soll in Kürze produktiv eingesetzt werden. Die mir vorliegenden Unterlagen lassen eine Verbesserung der technischen Maßnahmen erwarten. Aber auch in diesem Fall gilt, daß neue verbesserte Betriebssystemversionen eingesetzt werden müssen, wenn sie zur Verfügung stehen.

- Bei den Städtischen Kliniken Kassel und bei den Städtischen Kliniken Darmstadt gab es Probleme mit der Umsetzung einzelner Forderungen zur Benutzerkontrolle. Sowohl in Kassel als auch in Darmstadt muß ein Anwender bei der Anmeldung am System eine Benutzerkennung mit Passwort und beim Aufruf der Anwendung noch einmal ein Anwendungspasswort eingeben. Dabei wurde nicht geprüft, ob der Benutzer, der sich am System angemeldet hat, auch derjenige ist, dem das Anwendungspasswort zugeordnet ist. Eine Programmanpassung wird diesen Mangel beseitigen.

  Das Datenschutzkonzept verlangt, daß die Passworte der Benutzer verschlüsselt gespeichert werden müssen. Hiermit soll sichergestellt werden, daß nur die Person, der eine Benutzerkennung zugeordnet wurde, das zugehörige Passwort kennen kann. Bei den Städtischen Kliniken in Kassel konnte keines der Passworte verschlüsselt gespeichert werden. Um trotzdem einen weitgehenden Schutz gegen eine unbefugte Nutzung der Anwendung zu erreichen, wurde die Anwendung um zusätzliche Prüfungen erweitert. Dabei wird der Eingabebildschirm identifiziert und geprüft, ob er sich in den Sicherheitsbereichen SB1 oder SB2 befindet. Nur wenn das der Fall ist, kann die Anwendung aufgerufen werden. Zusammen mit den räumlichen Schutzmaßnahmen ist daher ein Minimalschutz erreicht. Trotzdem sind hier noch weitere Verbesserungen erforderlich.

  Bei den Städtischen Kliniken in Darmstadt entsprach die Benutzerkontrolle zwar auf der Systemebene den Forderungen des Datenschutz-Gesamtkonzeptes, nicht jedoch auf der Anwendungsebene. Durch die oben beschriebene Übergabe der Benutzerkennung von der Systemebene an die Anwendung, wird die Benutzerkontrolle von der Anwendung an das Betriebssystem verlagert. Das weiterhin einzugebende Anwendungs-Passwort hat dann die Funktion eines zusätzlichen Hindernisses und kann zur Verfahrenssteuerung verwendet werden. Hierdurch wird den Forderungen zur Benutzerkontrolle entsprochen.

- Es war in Kassel und in Darmstadt jedem Benutzer möglich, durch Drücken der „CRTL-Y"-Taste, auf die Systemebene zu gelangen. Da die Taste vom Hersteller zu diesem Zweck vorgesehen ist, sind tiefgehende Anpassungen nötig, um die Möglichkeit zu unterbinden.

- Bei der Kontrolle der Benutzerprofile konnte ich kleinere Unstimmigkeiten feststellen, die sofort beseitigt wurden. So waren Erfassungskräften beispielsweise Anwendungsfunktionen oder Datensatzarten zugeordnet, die nicht zu deren Aufgabenbereich gehörten. Es ergab sich daraus, daß die Benutzerprofile öfter und regelmäßig kontrolliert werden müssen.

- In Darmstadt war für alle Erfassungskräfte dieselbe Benutzerkennung eingetragen. Die Klinik hat meiner Forderung entsprechend umgehend jeder Erfassungskraft eine eigene Benutzerkennung gegeben.

- In Darmstadt gab es Probleme bei der Programmentwicklung. So war, durch personelle Engpässe bedingt, die Funktionstrennung nicht gegeben. Es fehlten auch Regelungen zur Programmentwicklung, die beispielsweise den Abschlußtest oder das Freigabeverfahren betrafen.

- Die bei den Städtischen Kliniken Darmstadt erstellten Protokolle waren nur schwer zu verstehen. Beispielsweise enthielt das Benutzeraktivitätenprotokoll die Angaben, wann welcher Benutzer welche Anwendungsfunktion aufgerufen hat. Da jedoch sowohl der Benutzer als auch die Anwendungsfunktion nur mit dem internen Schlüssel aufgelistet waren, war eine Kontrolle nur möglich, wenn die Benutzerliste und die Liste der Anwendungsfunktionen vorhanden war.

- In Darmstadt und in Kassel war der mir geschilderte Ablauf einer Fernwartung ausreichend sicher. In beiden Fällen existierte jedoch keine schriftliche Beschreibung der Abläufe, nach denen sich ein Mitarbeiter hätte richten können.

- Bei meiner Kontrolle der Besucherbücher habe ich Unstimmigkeiten bzw. Mängel festgestellt. Das Besucherbuch für den SB 1 wurde in Gießen im Sekretariat des Institutes im 3. Stock geführt. Nach Eintragung in das Besucherbuch erhielt der Besucher eine Code-Karte, mit der er sich den Zugang zum SB 1 selbst öffnen konnte.

Dieses Verfahren entspricht natürlich nicht dem Sinn eines Besucherbuches. Durch eine Ausgabe von Code-Karten und der Führung eines Besucherbuches im 3. Stock des Gebäudes konnte nicht lückenlos nachgewiesen werden, welche „betriebsfremden" Personen zu welchem Zeitpunkt das Rechenzentrum im Erdgeschoß des Gebäudes betreten haben. Gleichzeitig konnten mit der Person, die im Besucherbuch eingetragen war, noch mehrere Personen das Rechenzentrum betreten. Das Besucherbuch muß zukünftig innerhalb des Rechenzentrums durch besonders autorisierte Personen geführt werden, die die jeweilige Zutrittsberechtigung zu prüfen haben.

In Darmstadt und Kassel wurde kein Besucherbuch geführt.

5.1.3.2.2
Räumliche Mängel

- Im Datenschutz-Gesamtkonzept sind verschiedene Sicherungsmaßnahmen für die Räume, in denen die Rechner installiert sind, vorgeschrieben. Die Räume des SB 1, für die ein Closed-Shop einzurichten ist, waren in Kassel und Darmstadt jeweils durch angrenzende Büroräume zu erreichen, ohne daß die Zugänge verschlossen waren.

- In Darmstadt ist eine Einbruchmeldeanlage für die Räume des SB 1 installiert. Alarmmeldungen laufen beim Pförtner der Klinik auf. Der Pförtner war jedoch nicht darüber informiert, welche konkreten Maßnahmen er bei einem Alarm zu treffen hat.

  Es ist deshalb eine Dienstanweisung erforderlich, in der die bei einem Alarm zu treffenden Maßnahmen festgelegt sind. Zu den Maßnahmen habe ich dem Klinikum einige Vorschläge unterbreitet.

- In Kassel wurden die Schlüssel für die Räume des SB 3 nicht in allen Fällen restriktiv vergeben. So hatte z.B. ein Arzt, der keinen Zugriff auf die Daten des Tumorregisters haben durfte, noch einen Schlüssel für einen Raum des SB 3.

  Ich habe die sofortige Einziehung des Schlüssels gefordert.

5.1.3.3
Behebung der Mängel

Die Beseitigung der Mängel werde ich im Frühjahr 1991 überprüfen.

5.2
Gesundheits-Reformgesetz: Auseinandersetzungen um die Angabe der Diagnose auf dem Krankenschein

Eine Vielzahl von Anfragen, insbesondere von Patienten und Ärzten, habe ich im vergangenen Jahr zu der Frage erhalten, ob der Arzt die Diagnose auf dem Krankenschein angeben darf oder sogar muß. Das Problem hat auch in der Presse große Aufmerksamkeit gefunden.

Die im Gesundheits-Reformgesetz (GRG) vom 25. November 1988 getroffenen Regelungen lassen eine routinemäßige Übermittlung der Diagnose durch den Arzt nicht zu (zum GRG vgl. 17. Tätigkeitsbericht, Ziff. 6.1). Übermittelt ein Kassenarzt der Krankenkasse zum Zwecke der Abrechnung Daten über den versicherten Patienten, so liegt darin ein Eingriff in dessen verfassungsmäßiges Recht, selbst über die Verwendung seiner Daten zu bestimmen. Zugleich handelt es sich um eine Durchbrechung der ärztlichen Schweigepflicht i.S.v. § 203 Strafgesetzbuch. Der Arzt darf daher die Diagnose nur dann übermitteln, wenn eine Rechtsvorschrift dies erlaubt. Um dieser Rechtssituation Rechnung zu tragen, sind im GRG konkrete Regelungen zur Übermittlung von Patientendaten durch den Arzt an die Kassenärztlichen Vereinigungen bzw. an die Krankenkassen getroffen worden. In § 295 Abs. 1 Sozialgesetzbuch (SGB) V sind abschließend alle Daten aufgeführt, die der Arzt zur Abrechnung ärztlicher Leistungen an die Kassenärztliche Vereinigung bzw. an die Krankenkassen übermitteln muß und darf. Nach dieser Vorschrift ist der Arzt verpflichtet,

1.
in den Abrechnungsunterlagen für die kassen- und vertragsärztlichen Leistungen die von ihm erbrachten Leistungen einschließlich des Tages der Behandlung, bei zahnärztlicher Behandlung auch bezogen auf den einzelnen Zahn, aufzuzeichnen,

2.
in den Abrechnungsunterlagen sowie auf den Vordrucken für die kassen- und vertragsärztliche Versorgung seine Arztnummer sowie die Krankenversichertennummer des Patienten anzugeben.

Die Diagnose ist in § 295 Abs. 1 SGB V nicht genannt. Sie ist von den „erbrachten Leistungen" eindeutig zu unterscheiden. Anders ist die Rechtslage hinsichtlich der Krankenhäuser. In § 301 SGB V ist die Übermittlung der Aufnahme- und Entlassungsdiagnose neben sonstigen Angaben an die Krankenkasse ausdrücklich vorgesehen.

Der Arzt muß daher seine Schweigepflicht beachten und darf die Diagnose seiner Patienten nicht routinemäßig auf dem Krankenschein weitergeben. Auch die Hessische Kassenärztliche Vereinigung ist dieser Ansicht. Demgegenüber vertritt das Bundesarbeitsministerium in einer Stellungnahme vom 1. August 1990 die Auffassung, der Kassenarzt sei nach dem GRG zur Angabe der Diagnose auf dem Krankenschein verpflichtet. Das Bundesarbeitsministerium argumentiert, daß mit den vom Arzt anzugebenden von ihm erbrachten Leistungen auch die Diagnose gemeint sei. Als Folge der Stellungnahme des Bundesarbeitsministeriums haben die Spitzenverbände der Krankenkassen gegenüber der Kassenärztlichen Bundesvereinigung erkennen lassen, daß eine Honorarzahlung nur dann gewährleistet ist, wenn die Kassenärzte die Diagnose auf den Krankenscheinen vermerken. Die Hessische Kassenärztliche Vereinigung hat daraufhin allen hessischen Kassenärztinnen und Kassenärzten nahegelegt, bis zur endgültigen Klärung der Rechtslage die Diagnose auf dem Krankenschein weiterhin anzugeben.

Die Interpretation des Bundesarbeitsministeriums ist nicht vertretbar. Sie konterkariert das mit dem GRG angestrebte Ziel, die Verarbeitung der Patientendaten konkret zu regeln. Die sich aus der Stellungnahme des Ministeriums ergebende Rechtsunsicherheit ist unerträglich. Die Patienten sind verunsichert und die Ärzte in einer sehr schwierigen Lage. Die zum Schutz des informationellen Selbstbestimmungsrechts getroffenen Regelungen im GRG müssen ernst genommen werden. Der Bürger muß wissen, wer wann welche Daten zu welchen Zwecken über ihn verarbeitet. Sofern sich im Einzelfall eine Erweiterung getroffener Regelungen als notwendig erweist, kann dies nur der Gesetzgeber entscheiden.

6. Schulen

6.1
Überprüfung der Notengebung einzelner Lehrer

Die Zahl der Schulen, die für Verwaltungsaufgaben Personalcomputer einsetzen, ist in den letzten Jahren sprunghaft gestiegen. Ein typisches Beispiel, wie die Nutzung der automatisierten Datenverarbeitung auch die Kontrolle des Verhaltens einzelner Lehrer erleichtert, ist der folgende Fall:

An einer Gesamtschule, die mit mehreren anderen Schulen in einem Schulverbund zusammenwirkt, verfolgte der für die schulfachliche Koordination zwischen der Gesamtschule und den zugeordneten gymnasialen Oberstufen zuständige Lehrer mittels einer automatisierten Datei, wie sich beim Übergang von der Jahrgangsstufe 10 in die gymnasiale Oberstufe die Noten der Schüler einzelner Lehrer entwickelten. Der Schulleiter erhielt regelmäßig einen Ausdruck. In Auswertungen, die der Koordinator den Statistiken beifügte, wurden die Lehrkräfte, deren Schüler sich in der Jahrgangsstufe 11 erheblich verschlechtert hatten, als „bedenklich" eingestuft und es wurde davon abgeraten, die Betroffenen weiterhin in der 10. Jahrgangsstufe unterrichten zu lassen. Als weitere Folge sollen auch die von den betroffenen Lehrern gestellten Abordnungswünsche an die gymnasiale Oberstufe unberücksichtigt geblieben sein. Diese Kontrollpraxis führte zu mehreren Dienstaufsichtsbeschwerden gegen den Koordinator. Nachdem das Staatliche Schulamt die Beschwerden zurückgewiesen hatte, bat mich der interne Datenschutzbeauftragte der Gesamtschule, die datenschutzrechtliche Zulässigkeit derartiger Kontrollen zu überprüfen.

6.1.1
Zulässigkeit der Kontrollen

Zu den Aufgaben des Koordinators gehören u.a. die Information der Lehrer der Mittelstufenschulen und der Schulen der gymnasialen Oberstufen über die generelle Leistungsentwicklung von Schülern der jeweils anderen in die Koordinierung einbezogenen Schulen sowie die Beobachtung der generellen Leistungsentwicklung und Schullaufbahn der Schüler nach dem Stufenübergang und entsprechende Beratung (§ 32 Abs. 1 Nr. 3 und 4 Allgemeine Dienstordnung für Schulleiter, Lehrer und Erzieher vom 19. März 1981 – ABl. S. 199). Mit dem Wortlaut des Gesetzes sind auch fach- und klassenbezogene Leistungsbeobachtungen zu vereinbaren. Derart differenzierte Feststellungen über die Leistungsentwicklung der Schüler sind zwangsläufig gleichzeitig personenbezogene Feststellungen über die Notengebung einzelner Lehrer.

Stellt der Koordinator Fehlentwicklungen bei der Leistungsentwicklung fest, muß er den Schulleiter darüber informieren. Das gebietet seine gesetzliche Pflicht zu enger Zusammenarbeit. Der Schulleiter kann dann die erforderlichen administrativen Maßnahmen treffen, also etwa ein Gespräch mit dem betroffenen Lehrer führen, oder die Unterrichtsorganisation ändern. Dazu gibt ihm § 47 Abs. 2 Nr. 4 und Abs. 3 Schulverwaltungsgesetz die Möglichkeit, denn der Schulleiter stellt für die Lehrer verbindlich den Plan für die Unterrichtsverteilung sowie den Stunden- und Vertretungsplan auf. Er entscheidet über den Einsatz der Lehrer und muß sicherstellen, daß für jeden Unterricht die geeignete Lehrkraft eingesetzt wird.

Die Noten, die für die Leistungsbewertung der Schüler erhoben und gespeichert worden sind, werden zwar zu einem anderen Zweck verwendet (nämlich zur Leistungskontrolle der Lehrer), dies ist jedoch gem. § 13 Abs. 2 i.V.m. § 12 Abs. 2 Nr. 1 Hessisches Datenschutzgesetz zulässig, da die allgemeine Dienstordnung die zweckändernde Datenverarbeitung vorsieht.

Da öffentliche Stellen Daten ihrer Beschäftigten verarbeiten dürfen, wenn dies u.a. zur Durchführung innerdienstlicher organisatorischer und personeller Maßnahmen erforderlich ist (§ 34 Abs. 1 HDSG), bestehen somit gegen die beschriebene Kontrollpraxis keine datenschutzrechtlichen Bedenken.

Eine Verletzung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes ist nicht ersichtlich. Die generelle Überprüfung aller Lehrer der Schule wäre sicherlich unverhältnismäßig. Hier erfolgte jedoch eine Beschränkung auf die sachlich plausibel begründbare Überprüfung der Notengebung der Lehrer, die Schüler in Übergangsklassen zur gymnasialen Oberstufe unterrichteten.

6.1.2
Informationsansprüche der Betroffenen

Umstritten waren außerdem mögliche Informationsansprüche der Lehrer gegenüber der Schulleitung. Das Hessische Beamtengesetz gibt jedem Beamten das Recht auf Einsicht in seine vollständigen Personalakten (§ 107 Abs. 3). Zu den Personalakten zählen alle Unterlagen über die Person des Beamten unabhängig davon, ob sie in Haupt-, Neben- oder Sonderakten enthalten sind. Dieses Einsichtsrecht gilt auch für Personaldaten, die automatisiert gespeichert sind. Einsichtsrecht bedeutet in diesem Fall, daß die Daten lesbar gemacht werden müssen, was entweder durch einen Ausdruck oder an einem Datensichtgerät geschehen kann. Dem Beamten muß Gelegenheit gegeben werden, sämtliche ihn betreffenden Daten zur Kenntnis zu nehmen.

Für angestellte Lehrer ergibt sich das Einsichtsrecht aus § 13 Abs. 1 BAT.

Sieht man die von dem Koordinator geführte Datei und die Listen und Gutachten nicht als Personalakten an, könnten die Lehrer ihre Informationsansprüche auf das Hessische Datenschutzgesetz stützen (§ 18 Abs. 1 und 4, § 34 Abs. 3). Das Gesetz schreibt außerdem vor, daß Betroffene über die Speicherung ihrer Daten in automatisierten Dateien schriftlich zu benachrichtigen sind (§ 18 Abs. 2), d.h. Schulen, die solche Kontrollen automatisiert durchführen, müssen die betroffenen Lehrer unaufgefordert darüber informieren.

6.2
Elternbefragung des Kultusministeriums im Lahn-Dill-Kreis

6.2.1
Fragebogen und Erhebungsverfahren

Im Frühjahr 1990 erhielten die Eltern der Schüler der Klassen 4 der Grundschulen im Altkreis Wetzlar folgenden Fragebogen:

„Sollte zum Schuljahr 1990/91 im Altkreis Wetzlar ein Bildungsangebot Gymnasium, Realschule oder Hauptschule eingerichtet werden, bekunde ich hiermit mein Interesse, mein Kind für den Bildungsweg des/der

Gymnasiums
Realschule
Hauptschule

anzumelden.

Unterschrift des Erziehungsberechtigten"

Die Umfrage erfolgte auf Veranlassung des Kultusministeriums und wurde vom Staatlichen Schulamt des Lahn-Dill-Kreises durchgeführt. Das Staatliche Schulamt ließ die Erhebungsbögen von Schulleitern an die Eltern verteilen. Manche Schulleiter gaben die Bögen den Schülern mit nach Hause, andere schickten sie mit der Post an die Eltern. Die Schulen sollten die ausgefüllten Erhebungsvordrucke einsammeln und an das Staatliche Schulamt zur Auswertung weiterleiten.

Da die Befragung gleich aus mehreren Gründen gravierend gegen das Datenschutzrecht verstieß, mußte ich sie gegenüber dem Hessischen Kultusministerium förmlich beanstanden und die Löschung der bereits erhobenen Daten verlangen.

6.2.2
Umstrittene Zuständigkeit

Die Schulaufsichtsbehörde darf personenbezogene Daten nur im Rahmen ihrer rechtmäßigen Aufgabenerfüllung verarbeiten. Diese Voraussetzung war hier nach meiner Ansicht nicht erfüllt. Zweck der Erhebung war die Feststellung, ob ein öffentliches Bedürfnis für eine Änderung des bestehenden Bildungsangebots im Altkreis Wetzlar bestand. Es ging somit um eine Fortschreibung des Schulentwicklungsplanes. Die Errichtung von Schulen und die Aufstellung des Schulentwicklungsplanes sowie dessen Fortschreibung ist eindeutig Aufgabe des Schulträgers (§ 23 Abs. 2 und 5 Schulverwaltungsgesetz). Daran ändert auch die im Schulverwaltungsgesetz festgelegte Pflicht des Staates und der kommunalen Schulträger zur Zusammenarbeit nichts. § 23 Abs. 4 Schulverwaltungsgesetz sieht lediglich vor, daß die Schulentwicklungspläne und Beschlüsse des Schulträgers über Errichtung, Organisationsänderungen und Aufhebung von Schulen der Zustimmung des Kultusministeriums bedürfen. Dazu müssen

naturgemäß aber erst einmal Fortschreibungsentwürfe und Beschlüsse vorliegen. Die Datenerhebung konnte also allenfalls der Schulträger durchführen, was mitunter auch geschieht.

Das Kultusministerium ist dagegen der Meinung, daß es nicht um die Fortschreibung des Schulentwicklungsplanes ging. In einer ersten Stellungnahme teilte mir das Ministerium mit, die Schulaufsicht müsse tätig werden, wenn der Schulträger seiner Pflicht, je nach dem öffentlichen Bedürfnis bestimmte Bildungswege anzubieten, nicht nachkomme. Dem Lahn-Dill-Kreis sei in einem Urteil des Verwaltungsgerichtshofs vom Februar 1990 bestätigt worden, daß das im Kreis vorhandene Angebot schulformunabhängiger Gesamtschulen nicht alle Bildungswege umfasse und im Verhältnis zum gymnasialen Angebot keine ersetzende Wirkung habe. Schulaufsicht und Kommunalaufsicht hätten sich daher gem. § 65 Schulverwaltungsgesetz rüsten müssen, die Pflichten des Schulträgers durchzusetzen, falls dieser seinen aus dem Urteil des VGH folgenden Pflichten nicht nachgekommen wäre (die Vorschrift regelt das Aufsichtsverfahren bei Pflichtverletzungen des Schulträgers).

Ein Pflichtverstoß lag also nach dieser Darstellung des Ministeriums noch nicht vor. Als ich das Ministerium darauf hinwies, daß unter diesen Voraussetzungen die Umfrage eine Verarbeitung personenbezogener Daten auf Vorrat sei, um einem möglichen künftigen Rechtsverstoß des Schulträgers begegnen zu können, für Verwaltungszwecke jedoch keine personenbezogenen Daten auf Vorrat gespeichert werden dürften, wurde in einer zweiten Stellungnahme die Erhebung folgendermaßen begründet: Das Ministerium sei nicht nur gefordert, wenn der Schulträger seine Pflichten nicht erfülle, sondern auch dann, wenn er die Erfüllung seiner Pflichten schuldhaft verzögere. Der Schulträger habe mit einem Schreiben vom 15. März 1990 den Eindruck erweckt, er beabsichtige Verzögerungen in einem nicht mehr vertretbaren Maße. Dazu paßt allerdings nur schwer, daß das Staatliche Schulamt bereits mit Schreiben vom 12. März 1990 den Schulleitern die Erhebungsbögen zuschickte und zur Durchführung der Befragung aufforderte und dabei Bezug auf zwei Erlasse vom Februar 1990 nahm.

6.2.3
Unnötige Verarbeitung personenbezogener Daten

Gleichgültig welchen Erhebungszweck man unterstellt, gemessen an beiden wurden jedenfalls unnötigerweise personenbezogene Daten verarbeitet, so daß die Befragung auch aus diesem Grund rechtswidrig war. Die überflüssige Datenverarbeitung verstieß sowohl gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit als auch gegen § 11 Abs. 1 Hessisches Datenschutzgesetz. Das Bundesverfassungsgericht hat im Volkszählungsurteil von 1983 klargestellt, daß sich alle öffentlichen Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, dabei „auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen" (BVerfGE 65, 46). Diesen Grundsatz enthält auch das Hessische Datenschutzgesetz in der zitierten Vorschrift. Die Elternbefragung hätte ohne Informationsverlust problemlos in anonymisierter Form durchgeführt werden können. Eine offensichtlich unnötige Verarbeitung personenbezogener Daten ist nach der Rechtsprechung des Bundesverfassungsgerichts und dem Hessischen Datenschutzgesetz selbst mit Einwilligung der Betroffenen nicht zulässig.

Das Ministerium wollte durch den Personenbezug sicherstellen, daß nur diejenigen Erziehungsberechtigten ihre Wünsche äußerten, für die eine Wahlentscheidung anstand. Das war aber bereits durch die Gestaltung des Erhebungsverfahrens weitgehend garantiert. Lediglich in den Fällen, in denen die Schulleitungen die Erhebungsvordrucke an die Schüler aushändigten, waren Manipulationen nicht gänzlich ausgeschlossen. Die 10jährigen Schüler hätten z.B. den Erhebungsbogen nicht den Erziehungsberechtigten aushändigen, den ausgefüllten Erhebungsbogen nicht in der Schule abgeben oder den Bogen selbst ausfüllen bzw. sich durch Dritte ausfüllen lassen können. Es fällt schwer, sich ein Motiv für eine dieser Möglichkeiten vorzustellen. Die geringe Fehlerquote, die hier zu erwarten war, hätte das Ergebnis kaum verfälscht. Um jedoch jedes Risiko auszuschließen, hätte es genügt, wenn die Schulleitungen die Erhebungsbögen den Erziehungsberechtigten ausschließlich mit der Post zugesandt und diese die ausgefüllten Fragebögen anonymisiert per Post an das Staatliche Schulamt zurückgeschickt hätten. Es war somit absolut kein Grund für eine personenbezogene Datenerhebung ersichtlich.

Für eine überflüssige und damit unzulässige Datenverarbeitung sprach außerdem die vom Kultusministerium unwidersprochen gebliebene Darstellung des Landrats des Lahn-Dill-Kreises, die Schulaufsicht habe keinen Anlaß zu der Annahme gehabt, der Schulträger gehe davon aus, es gäbe nicht genügend interessierte Eltern für ein gymnasiales Bildungsangebot. Die Schulaufsicht habe sich vor der Befragung nicht einmal erkundigt, von welchen Daten der Schulträger ausgehe und ob überhaupt eine unterschiedliche Einschätzung bestehe.

Da es in der Auseinandersetzung zwischen Ministerium und Schulträger gar nicht um die Errichtung von Real- und Hauptschulen ging, sondern um Gymnasien, war die Erhebung der ersten beiden Daten darüber hinaus aus einem weiteren Grund nicht erforderlich und deshalb unzulässig.

6.2.4
Verletzung der Informationspflichten

Die Elternbefragung verstieß aber noch aus einem anderen Grund gegen das Datenschutzrecht: Die in den §§ 7 Abs. 2 und 12 Abs. 4 Hessisches Datenschutzgesetz festgelegten Unterrichtungspflichten der datenverarbeitenden Stelle waren nicht eingehalten worden. Nach diesen Bestimmungen mußten die Erziehungsberechtigten über den Zweck der Erhebung, die Art der Datenverarbeitung (manuell oder automatisiert), die Dauer der Datenspeicherung und etwaige Übermittlungen aufgeklärt werden. Außerdem waren die Betroffenen auf die Freiwilligkeit der Teilnahme

hinzuweisen und darauf, daß aus einer Verweigerung keine Rechtnachteile entstehen würden. Die Erhebungsunterlagen enthielten keine derartigen Informationen. Die Fragebögen ließen nicht einmal erkennen, welche Stelle die Daten erhob und weiterverarbeitete.

Das Kultusministerium sandte mir als Beleg für die Einhaltung der Informationspflichten die Kopie eines Begleitschreibens, das der Rektor einer Schule den Fragebögen beigefügt hatte. Seltsamerweise fand sich in dem Schreiben kein einziger der vom Gesetz geforderten Hinweise. Die Entscheidung über das Ob und Wie der Unterrichtung war den Schulleitern überlassen. In mehreren mir bekannt gewordenen Fällen gab es überhaupt kein Begleitschreiben. Mündliche Erläuterungen, die vielleicht in Einzelfällen den 10jährigen Schülern gegeben wurden, konnten jedoch auf keinen Fall die unmittelbare Information der Erziehungsberechtigten ersetzen.

Nach Auffassung des Ministeriums ergab sich der Erhebungszweck außerdem aus dem Erhebungsbogen selbst und soll jedem, der die öffentliche Diskussion im Altkreis Wetzlar verfolgt hat, klar gewesen sein. Letzteres scheint, gerade wenn man den vom Kultusministerium behaupteten Zweck unterstellt, schon in tatsächlicher Hinsicht äußerst zweifelhaft. Es dürfte nicht nur ausländischen Erziehungsberechtigten schwergefallen sein, aus der Berichterstattung der Medien zu erkennen, daß die Erhebung der Vorbereitung aufsichtsrechtlicher Maßnahmen gegen den Schulträger dienen sollte. Wichtiger ist jedoch: Die Unterrichtungsregeln des Hessischen Datenschutzgesetzes sind keine Ermessensvorschriften. Die Erfüllung dieser Bestimmungen wird nicht dadurch entbehrlich, daß ein aufmerksamer Zeitungsleser oder Rundfunkhörer möglicherweise über den Zweck der Erhebung informiert sein konnte. Es genügt auch nicht, daß sich Zweck der Erhebung oder Freiwilligkeit der Teilnahme irgendwie aus den Erhebungsbögen indirekt erkennen lassen, sondern das Gesetz verlangt positive Hinweise, die hier jedoch nicht erfolgt waren.

6.2.5
Zweifel des Kultusministeriums am Personenbezug

Verwunderlich war der in der Stellungnahme des Kultusministeriums enthaltene Hinweis, der Personenbezug komme ausschließlich in einer eigenhändigen Unterschrift zum Ausdruck, andere „persönliche" Daten seien im Erhebungsbogen nicht erfaßt worden. Damit sollte anscheinend die Geltung des Hessischen Datenschutzgesetzes im vorliegenden Fall in Frage gestellt werden. Zum einen wurden sehr wohl mehr personenbezogene Daten als nur die Namen der Betroffenen erhoben, nämlich die Informationen „Erziehungsberechtigter eines Schülers oder einer Schülerin der 4. Klasse im Altkreis Wetzlar" und „Entscheidung für Gymnasium, Realschule oder Hauptschule". Zum anderen ist es für die Geltung des Hessischen Datenschutzgesetzes unerheblich, ob der Personenbezug nur in einer Unterschrift zum Ausdruck kommt. Die Daten sind personenbezogen. Das HDSG gilt für die Verarbeitung aller personenbezogenen Daten. Es unterscheidet z.B. nicht zwischen sensitiven oder weniger sensitiven Daten. In diesem Zusammenhang gilt es an die Bemerkung des Bundesverfassungsgerichts zu erinnern, daß es unter den Bedingungen der automatisierten Datenverarbeitung keine „belanglosen" Daten mehr gibt (BVerfGE 65, 45).

6.2.6
Behandlung im Landtag

Die Erhebungsunterlagen wurden zwar unausgewertet vernichtet. Das Ministerium teilte mir jedoch mit, daß dafür nicht die von mir geltend gemachten datenschutzrechtlichen Bedenken ausschlaggebend gewesen seien, sondern die Zusicherung des Schulträgers, innerhalb eines festgelegten Zeitplanes für ein gymnasiales Bildungsangebot zu sorgen.

Die Befragung und besonders die Kontroverse zwischen dem Kultusministerium und dem Hessischen Datenschutzbeauftragten hat zu mehreren Anträgen der Opposition im Landtag geführt (Drucks. 12/6403, 12/6409 und 12/6461). Das Ministerium ist auch in seiner schriftlichen Stellungnahme vom 27.08.1990 für den Unterausschuß Informationsverarbeitung und Datenschutz bei seiner Rechtsauffassung geblieben, daß die Befragung rechtmäßig war. Die Behandlung im Ausschuß steht noch aus.

6.3
Richtlinien für den Datenschutz in Schulen

6.3.1
Notwendigkeit schulspezifischer Datenverarbeitungsregelungen

Im Januar 1990 hat mir das Kultusministerium einen Richtlinienentwurf für den Datenschutz in Schulen zur Stellungnahme vorgelegt. Nicht nur in den datenschutzrechtlichen Fortbildungsveranstaltungen für Schulleiter, schulische Datenschutzbeauftragte und Schulpersonalräte, sondern auch in vielen Anfragen, die ich in den letzten Jahren aus den Schulen erhalten habe, wurde immer wieder deutlich, wie dringend notwendig konkretisierende Datenschutzvorschriften im Schulbereich sind.

So hilfreich eine Richtlinie zweifelsohne ist, so wenig kann sie freilich die für die Verarbeitung personenbezogener Schüler- und Elterndaten fehlende gesetzliche Grundlage ersetzen. Jede Verarbeitung personenbezogener Daten durch die Schulen ist ein Eingriff in das verfassungsrechtlich garantierte informationelle Selbstbestimmungsrecht der Betroffenen. Dieser Eingriff ist nur auf einer gesetzlichen Grundlage zulässig. Das gilt unabhängig vom Grad der Einschränkung oder der Intensität der Belastung der Betroffenen. Die beiden Kriterien sind allerdings entscheidend

für die Ausgestaltung der notwendigen gesetzlichen Grundlage, d.h. Art, Umfang und Regelungsdichte der gesetzgeberischen Maßnahmen müssen sich an der jeweiligen Datenverarbeitung orientieren. Für schwerwiegende Einschränkungen sind die allgemeinen Verarbeitungsregelungen des Hessischen Datenschutzgesetzes in Verbindung mit einer gesetzlichen Aufgabenzuweisung keine ausreichende gesetzliche Grundlage, es sind vielmehr bereichsspezifische Befugnisnormen erforderlich. Zu den schwerwiegenden Eingriffen zählt das Bundesverfassungsgericht ausdrücklich die Fälle, in denen der Staat die Angabe personenbezogener Daten vom Bürger verlangt. „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind." (BVerfGE 65, 45, 46).

Der Erlaßentwurf geht davon aus, daß die Schüler und Erziehungsberechtigten aufgrund des Schulverhältnisses und des Schulpflicht- und Schulverwaltungsgesetzes sowie aufgrund der zur Durchführung dieser Gesetze erlassenen Rechtsvorschriften verpflichtet sind, die von der Schule für die Erfüllung der jeweiligen Aufgaben benötigten Daten anzugeben. Mit der beschriebenen Rechtsprechung des Bundesverfassungsgerichts ist dies jedoch nicht zu vereinbaren.

Der zwangsweisen Datenerhebung stehen die Fälle gleich, in denen es zu den Obliegenheiten des Betroffenen gehört, Auskünfte im Zusammenhang mit Leistungen zu erteilen, von denen er abhängig ist. Der nicht mehr schulpflichtige Schüler darf nicht schlechter gestellt werden als der schulpflichtige, denn ersterer ist praktisch ebenfalls gezwungen, der Schule seine Daten mitzuteilen, will er nicht auf das Bildungsangebot ganz verzichten.

Ein schwerwiegender Eingriff liegt auch dann vor, wenn die Datenerhebung ohne Wissen und Willen des Betroffenen erfolgt (z.B. durch Befragung Dritter) oder wenn sensible personenbezogene Daten, wie beispielsweise Gesundheitsdaten, erhoben werden.

Lediglich für die Verarbeitung der Beschäftigtendaten in der Schule ist mit § 34 Hessisches Datenschutzgesetz eine ausreichende bereichsspezifische Grundlage vorhanden.

Daraus folgt: Eine gesetzliche Regelung ist auf jeden Fall für die Datenverarbeitung im Rahmen der Schulgesundheitspflege und des schulpsychologischen Dienstes erforderlich. § 42 Schulverwaltungsgesetz und § 17 Schulpflichtgesetz, die den betroffenen Schülern bzw. Erziehungsberechtigten lediglich eine Duldungs- und Auskunftspflicht auferlegen, reichen nicht aus. Es müßte außerdem für die übrige Datenverarbeitung in den Schulen zumindest eine datenschutzrechtliche Grundnorm in das Schulverwaltungsgesetz aufgenommen werden, die eine Verordnungsermächtigung enthalten könnte, so daß eine Konkretisierung im Wege einer Rechtsverordnung möglich wäre. Damit würde Hessen im übrigen auch Anschluß an andere Bundesländer gewinnen: Das Land Bremen hat mittlerweile ein Gesetz zum Datenschutz im Schulwesen. Die Länder Bayern, Rheinland-Pfalz, Saarland, Nordrhein-Westfalen und Schleswig- Holstein haben bereichsspezifische Vorschriften in ihre Schulverwaltungsgesetze aufgenommen oder in Vorbereitung.

Auch ein Vergleich der Datenverarbeitung in Schulen mit der Situation in anderen Bereichen der Landesverwaltung zeigt die Notwendigkeit gesetzlicher Regelungen. Es ist nämlich nicht einzusehen, daß der Gesetzgeber, wie jüngst durch die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG), die Datenverarbeitung der Polizei detailliert regelt, aber den Schulbereich, in dem häufig nicht minder sensitive Daten verarbeitet werden, ohne bereichsspezifische gesetzliche Vorgaben läßt. Für die Schulen kann schließlich auch kein geringerer Standard als etwa für die Hochschulen gelten, deren Studentendatenverarbeitung das Hessische Ministerium für Wissenschaft und Kunst kürzlich durch die neue Immatrikulationsverordnung ebenfalls weitgehend bereichsspezifisch geregelt hat (vgl. 17. Tätigkeitsbericht, Ziff. 8.1).

Seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 sind inzwischen sieben Jahre vergangen. Der Übergangsbonus kann aber nicht zeitlich unbegrenzt in Anspruch genommen werden. Deshalb müssen in der nächsten Legislaturperiode zu den ersten Gesetzgebungsvorhaben bereichsspezifische Regeln für den Schulbereich gehören.

6.3.2
Inhalt der Richtlinien

Von den zahlreichen Verarbeitungsbedingungen, die der Entwurf vorsieht, werden im folgenden nur einige erwähnt, die typische und immer wiederkehrende Unsicherheiten und Streitpunkte behandeln.

6.3.2.1
Datenkatalog

Da nach der Rechtsprechung des Bundesverfassungsgerichts und dem Hessischen Datenschutzgesetz öffentliche Stellen nur die personenbezogenen Daten verarbeiten dürfen, die sie zur Aufgabenerfüllung benötigen, definiert der Richtlinienentwurf präzise, welche Daten über Schüler, Erziehungsberechtigte und Lehrer die Schulen verarbeiten dürfen. Der Datensatz der Schüler umfaßt neben den Individualdaten des Schülers, Organisations-, Schullaufbahn- sowie Leistungs- und Prüfungsdaten. Differenziert nach Grundschulen, gymnasialen Oberstufen, berufliche Schulen und Sonderschulen legt der Entwurf außerdem die erforderlichen schulformspezifischen Schülerdaten fest. Damit

erhalten die Schulen einen – wie die Erfahrung zeigt – dringend benötigten Verarbeitungsrahmen. Fälle, in denen Schulen z.B. bei der Einschulung von den Eltern aller Kinder einen umfangreichen Fragebogen ausfüllen lassen, in dem u.a. nach den Wohnverhältnissen, Krankheiten und psychischen Dispositionen gefragt wird, dürften danach eigentlich nicht mehr vorkommen.

Der Entwurf beseitigt außerdem die vielfach bei den Schulen anzutreffende Unsicherheit darüber, welche personenbezogenen Daten automatisiert verarbeitet werden dürfen. In einer Übersicht sind sowohl die Schüler- als auch die Eltern- und Lehrerdaten abschließend aufgezählt, die im Schulcomputer gespeichert werden dürfen. Nicht dazu zählen beispielsweise Daten über gesundheitliche Auffälligkeiten und Behinderungen des Schülers und Angaben über besondere pädagogische, soziale und therapeutische Maßnahmen und deren Ergebnisse.

Mit der Auflistung der Daten, die im Klassenbuch vermerkt werden dürfen, schafft die Richtlinie in einem weiteren häufig auftretenden Streitpunkt Klarheit. Leistungsdaten zählt sie ausdrücklich nicht zum zulässigen Inhalt.

6.3.2.2
Interner Datenschutzbeauftragter

Ausführlich widmet sich der Richtlinienentwurf dem schulischen Datenschutzbeauftragten. Er beschreibt das Bestellungsverfahren und konkretisiert Aufgaben und rechtliche Stellung des internen Datenschutzbeauftragten. Durchaus zutreffend geht der Entwurf davon aus, daß der interne Datenschutzbeauftragte primär eine beratende Funktion hat. Kontrollbefugnisse weist ihm das Hessische Datenschutzgesetz nur zu, soweit es um die Einhaltung der erforderlichen technischen und organisatorischen Datensicherheitsmaßnahmen geht.

6.3.2.3
Nutzung von Personal Computern außerhalb der Schule für dienstliche Zwecke

Einem besonders starken Regelungsbedürfnis der Schulen entsprechen zweifellos die Bestimmungen zur Nutzung von PC's für dienstliche Aufgaben außerhalb der Schule.

Der Entwurf läßt die Verarbeitung von Schülerdaten auf Rechnern außerhalb der Schule nur zu, wenn der Lehrer die Daten zur Erfüllung der in seinem unmittelbaren Verantwortungsbereich liegenden pädagogischen Aufgaben benötigt und zählt dazu Namen der Schüler und Aufzeichnungen über Leistungen. Daten, die in Schülerakten, Klassenbüchern und Dateien der Schule zu erfassen sind oder schulische Veranstaltungen, wie z.B. die Durchführung eines Betriebspraktikums betreffend, unterliegen nach dem Entwurf nicht dem Verantwortungsbereich des Lehrers und dürfen daher nicht außerhalb der Schule verarbeitet werden.

Da Lehrern in der Schule regelmäßig kein eigener Arbeitsplatz für die Erledigung von Verwaltungsaufgaben zur Verfügung steht, sondern sie ein Teil ihrer dienstlichen Tätigkeit zu Hause leisten, dürfen sie in dem für die Aufgabenerfüllung notwendigen Umfang folglich auch außerhalb der Schule personenbezogene Daten verarbeiten. Erforderlich erscheint jedoch nur eine Verarbeitung von Schülerdaten. Elterndaten, soweit sie beispielsweise für Benachrichtigungen benötigt werden, lassen sich jederzeit im Schulsekretariat erfragen.

Der Entwurf läßt die Verarbeitung personenbezogener Schülerdaten auf Rechnern außerhalb der Schule mit Recht nur unter eingeschränkten Voraussetzungen zu. Wegen der wesentlich größeren Gefährdung, die die automatisierte Datenverarbeitung gegenüber der manuellen für das informationelle Selbstbestimmungsrecht der Schüler bedeutet, habe ich dem Kultusministerium in meiner Stellungnahme jedoch die Aufnahme zusätzlicher Bedingungen empfohlen:

- Es ist zu betonen, daß die Schule speichernde Stelle der Daten ist, die auf dem Rechner außerhalb der Schule verarbeitet werden. Die Schule muß die Daten an das Dateienregister des Hessischen Datenschutzbeauftragten melden.

- Die Schülerdaten, die die Lehrer außerhalb der Schule automatisiert verarbeiten dürfen, sollten in der Richtlinie abschließend aufgezählt werden.

- Lehrer, die zur Erledigung schulischer Aufgaben in Privaträumen Schülerdaten auf einem Rechner verarbeiten wollen, müssen dazu die Genehmigung des Schulleiters einholen.

- Die Genehmigung darf nur erteilt werden, wenn sich der Lehrer schriftlich mit einer etwaigen Kontrolle durch den Hessischen Datenschutzbeauftragten einverstanden erklärt.

- Der Schulleiter erhält eine Dokumentation des Verfahrens, in der der Zweck der Verarbeitung, die eingesetzten Programme und die verarbeiteten Dateien beschrieben werden.

- An technischen und organisatorischen Maßnahmen sind im Fall der Nutzung von dienstlichen Rechnern die Maßnahmen zu treffen, die auch in der Schule vorgesehen würden. Werden private Rechner eingesetzt, so dürfen die Programme und Daten, die für dienstliche Zwecke verwendet werden, nur auf für diesen Zweck von der Schule gestellten beweglichen Datenträgern gespeichert werden. Diese Datenträger sind gesondert aufzube-

wahren. (Mit dieser Vorschrift soll verhindert werden, daß Lehrer über ihr Eigentum an den Datenträgern Ansprüche an den dienstlichen Daten geltend machen können.)

6.3.3
Verzögerungen

Nach mehrjähriger Vorbereitung sollte der Erlaß eigentlich im Sommer oder spätestens im Frühherbst 1990 veröffentlicht werden, so sah jedenfalls der Zeitplan des Kultusministeriums noch im Frühjahr aus. Zwischenzeitlich ist es jedoch zwischen dem Ministerium und dem Hauptpersonalrat zu einer Kontroverse über die Bestimmungen zur Personaldatenverarbeitung gekommen. Eine Lösung dieses Konflikts ist nach Ansicht des Ministeriums im Augenblick nicht in Sicht, so daß auf den Erlaß wohl noch einige Zeit zu warten sein wird.

7. Polizei

7.1
Abschließende Novellierung des HSOG

7.1.1
Ausweitung der polizeilichen Befugnisse

Nachdem der Hessische Gesetzgeber zum 1. Januar 1990 die von mir immer wieder angemahnten gesetzlichen Vorschriften zur polizeilichen Datenverarbeitung in Kraft gesetzt hat, war der Auftrag des Bundesverfassungsgerichts nach dem Volkszählungsurteil aus dem Jahr 1983 im wesentlichen erfüllt (Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 18. Dezember 1989 – GVBl I S. 469): Durch die Novellierung wurde die polizeiliche Datenverarbeitung erstmalig unter Datenschutzgesichtspunkten geregelt.

Allerdings hatte der Gesetzgeber bereits bei der Verabschiedung der Novelle im Jahre 1989 deutlich gemacht, daß im Rahmen einer Gesamtrevision des HSOG eine Überarbeitung auch dieser Datenverarbeitungsvorschriften vorgenommen würde. Insbesondere die Regelung des § 44d (Datenerhebung durch Einsatz von Personen, deren Zusammenarbeit mit der Vollzugspolizei Dritten nicht bekannt ist) wurde für korrekturbedürftig gehalten.

Die Gesamtrevision ist mittlerweile mit dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung vom 26. Juni 1990 (GVBl. I S. 197) erfolgt. Das Gesetz ist am 01.01.1991 in Kraft getreten. Neben einer veränderten Paragraphenfolge enthält die Neufassung des HSOG vor allem redaktionelle Verbesserungen. Von einer Ausnahme abgesehen, ist der Inhalt im wesentlichen unverändert geblieben. Meine Kritik im 18. Tätigkeitsbericht (Ziff. 4.1.1) ist nicht berücksichtigt worden.

Die einzige bedeutsame inhaltliche Änderung, die Neufassung des bisherigen § 44d durch § 16 HSOG vom 26. Juni 1990 ist keine datenschutzrechtliche Verbesserung, sondern im Gegenteil eine erhebliche Verschlechterung. Die Vorschrift stand daher im Mittelpunkt meiner Stellungnahmen, die ich im Laufe des Gesetzgebungsverfahrens vor den zuständigen Landtagsausschüssen abgegeben habe. Neben V-Leuten dürfen künftig auch verdeckte Ermittler, das sind Polizeibeamte, die unter einer sogenannten „Legende" (einem fingierten Lebenslauf) tätig sind, zur Gefahrenabwehr eingesetzt werden. Die alte Bestimmung ließ den Einsatz von V-Personen nur zu bei Straftaten mit erheblicher Bedeutung auf dem Gebiet des unerlaubten Betäubungsmittel- oder Warenverkehrs, der Geld- oder Warenzeichenfälschung und auf dem Gebiet des Staatsschutzes, die gewerbs- oder gewohnheitsmäßig oder von einem Bandenmitglied oder in anderer Weise organisiert begangen werden sollten. Nach der Neuregelung genügt für den Einsatz von V-Personen und verdeckten Ermittlern, daß irgendeine Straftat mit erheblicher Bedeutung in der beschriebenen Form begangen werden soll.

7.1.2
Bewertung des § 16 HSOG

7.1.2.1
Verfassungswidriger Anwendungsbereich

Eine datenschutzrechtliche Bewertung des neuen § 16 HSOG muß sich an den Grundsätzen der polizeilichen Datenverarbeitung orientieren. Demnach hat die Erhebung personenbezogener Daten regelmäßig offen und bei der betroffenen Person zu erfolgen. Der Bürger soll feststellen und überprüfen können, ob und in welchem Umfang die Polizei Daten über ihn erhebt und weiterverarbeitet. Verdeckte Ermittlungen verletzen diesen Grundsatz. Denn sowohl bei der verdeckten Weitergabe von Daten als auch bei der Verwendung einer Legende täuscht der Ermittler denjenigen, dessen Daten er erhebt und weitergibt. Diese Täuschung kann bis in die unmittelbare Privatsphäre hineinreichen, insbesondere dann, wenn auch – was das Gesetz ausdrücklich zuläßt – Daten aus der Wohnung des Betroffenen erhoben werden dürfen. Eine solche verdeckte Weitergabe auch intimer Lebensumstände an Polizeidienststellen ist zweifellos ein gravierender Eingriff, zumal diese Erhebung zu polizeilichen Sanktionen führen kann. Hinzu kommt, daß in dem neuen § 16 ausdrücklich auch auf die Möglichkeit des Einsatzes technischer, d.h. akustischer und optischer Hilfsmittel (Telefonabhören, Einsatz von Richtmikrofonen oder Tonbandaufnahmen) verwiesen wird und damit den Umständen nach auch vorläufige und auf Vergänglichkeit ausgerichtete

Lebensäußerungen zu Beweis- und Ermittlungszwecken aufgezeichnet werden dürfen. Die Tätigkeit sowohl von V-Personen als auch verdeckten Ermittlern greift tief in die Persönlichkeitssphäre der Betroffenen ein. Aus diesem Grund sollte sie nur in besonderen, genau eingegrenzten und begründeten Ausnahmefällen erfolgen dürfen.

Ein solcher besonderer Fall liegt wohl dann vor, wenn die üblichen polizeilichen Informationsmittel aufgrund von Organisationsstrukturen der „Gegenseite" nicht mehr funktionieren. Wo organisierte Straftäter arbeitsteilig und unter Androhung von Gewalt gegenüber Zeugen bzw. Informanten faktisch eine geschlossene, nur schwer von außen durchdringbare Kriminalitätsstruktur entwickeln, kann der Einsatz solcher Erhebungsmethoden legitim sein.

Der Hessische Gesetzgeber sieht diese Voraussetzungen aber nicht nur für den Bereich der Rauschgiftkriminalität, der Schutzgelderpressung, des illegalen Waffenhandels oder vergleichbar schwere Kriminalität für gegeben an. Im Gegensatz zu der bis zum 01.01.1991 geltenden Bestimmung knüpft die neue Vorschrift nur an den Begriff „Straftaten mit erheblicher Bedeutung" an. Der Anwendungsbereich für diesen besonders schwerwiegenden Eingriff ist damit viel zu weit gefaßt. Die Norm ist deshalb verfassungswidrig.

Sie ist auch aus folgenden Gründen verfassungswidrig: Die Formulierung des Gesetzes, die „insbesondere" dann, wenn Straftaten mit erheblicher Bedeutung drohen, den Einsatz von V-Personen und verdeckten Ermittlern zuläßt, weitet den Anwendungsbereich der Norm noch aus. Sie eröffnet die Möglichkeit, ggf. noch andere Straftatbestände einzubeziehen. Damit werden große Deliktsgruppen für den Einsatz verdeckt tätiger Personen eröffnet, ohne daß eine entsprechende Notwendigkeit aus polizeilicher Sicht eindeutig nachgewiesen worden wäre.

Der Gesetzgeber unterscheidet auch nur formal nach den Personenkreisen „verantwortlicher Störer, Person aus dem unmittelbaren Umfeld und weitere Personen". Die gesetzliche Bestimmung führt dazu, daß letztlich auch nur ein loser Zusammenhang zu einem bestimmten Ereignis zu einer Datenerhebung führen kann. Mit anderen Worten, es könnte auch so formuliert werden: „Personenbezogene Daten können mit Hilfe von V-Personen erhoben werden, wenn dies aufgrund tatsächlicher Anhaltspunkte für die Verhütung von Straftaten mit erheblicher Bedeutung erforderlich ist."

7.1.2.2
Befugnisse der verdeckten Ermittler

Aber auch die Befugnisse der verdeckt ermittelnden Personen läßt das Gesetz weitgehend im unklaren. Insbesondere das Problem des Einsatzes von optischen und akustischen Hilfsmitteln bleibt weitgehend offen. In einer Ausnahmevorschrift (Abs. 6) gelten die einschränkenden Absätze 2 bis 5 des § 15 (Datenerhebung durch Observation und Einsatz technischer Mittel) gerade nicht, wenn das Abhören zur Eigensicherung einer V-Person oder eines verdeckten Ermittlers geschieht. Durch die bloße Negativabgrenzung können zum Zweck der Eigensicherung Daten durch Abhören faktisch ohne Einschränkung erhoben werden. Nicht einmal der Erforderlichkeitsgrundsatz als Grundregel der personenbezogenen Datenverarbeitung wird in der Bestimmung verankert. Auch eine Zweckbindung der auf diese Weise erhobenen Daten fehlt. § 15 Abs. 6 läßt absolut offen, was mit diesen, durch technische Hilfsmittel gewonnenen Daten geschehen darf. Dies ist ein Verstoß gegen die verfassungsrechtlichen Vorgaben der Bestimmtheit, der Normentransparenz und der Verhältnismäßigkeit.

7.1.2.3
Gesetzentwurf des Bundesrats

Dieser Wertung steht auch nicht entgegen, daß der Bundesrat in einem „Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG – Bundesrats-Drucks. 74/90)", mit dem auch die Strafprozeßordnung um entsprechende Vorschriften angereichert werden soll, den Einsatz verdeckter Ermittler im Ergebnis in eben diesem Umfang zulassen möchte. Gegenüber dem Entwurf des Bundesrates fallen aber zwei wesentliche Unterschiede auf: Zum einen sieht dieser Entwurf den Einsatz von sogenannten V-Personen nicht vor, sondern legt in der Begründung (S. 67 der Drucksache) ausdrücklich dar, daß die Vorschläge keine Regelung für die Inanspruchnahme von Informanten sowie über den Einsatz von Vertrauenspersonen (V-Personen) vorsehen. Der Bundesrat behandelt diese Personen strafprozessual vielmehr als Zeugen, so daß die notwendige gesetzliche Grundlage für ihre Heranziehung im Ermittlungs- und Strafverfahren gegeben ist, soweit sie aufgrund ihrer Wahrnehmungen gefährdet sind, kommt ihnen derselbe Zeugenschutz zu, wie den Zufallszeugen. Hinsichtlich der Zusicherung der Vertraulichkeit/Geheimhaltung enthält bereits die o.g. bundeseinheitliche Richtlinie von 1986 Regelungen, die auf dem geltenden Recht beruhen und sich bewährt haben (Anmerkung: gemeint sind die Richtlinien der Justiz- und Innenressorts der Länder aus dem Jahr 1986 über den Einsatz von verdeckten Ermittlern und V-Personen). Damit wird für den Bundesbereich überzeugend der Verzicht auf Sonderregelungen für den Einsatz von V-Personen begründet.

Zum anderen kommt für die hessische Regelung hinzu, daß weder der Einsatz von V-Personen noch von verdeckten Ermittlern für den präventiven Bereich bisher ausreichend begründet worden ist. Auch Polizeipraktiker halten vielfach solche Maßnahmen zu präventiven Zwecken für entbehrlich. Denn bei der sogenannten organisierten Kriminalität handelt es sich in der Regel um Straftaten, die mit „Organisationsdelikten" verknüpft sind. Bei diesen Tatbeständen steht bereits die Bildung einer kriminellen Gruppierung unter Strafandrohung. Dadurch wird die Strafbarkeit „vorverlagert", so daß schon sehr früh ein strafprozessual verwertbarer Verdacht angenommen werden kann. Deshalb kann in aller Regel bereits auf repressive Normen aus der Strafprozeßordnung zurückgegriffen

werden, wenn die Entscheidung gefällt werden muß, ob ein Einsatz von V-Personen oder verdeckten Ermittlern erforderlich erscheint.

7.2
Erkenntnisanfrage über einen Sozialhilfebetrüger

Das Polizeipräsidium Wiesbaden forderte Anfang 1990 die Sozialministerien aller Bundesländer auf, die ihnen nachgeordneten Sozialämter zu bitten, „eine Auflistung über alle Sozialleistungen", die eine bestimmte Person erhalten hatte, dem Polizeipräsidium mitzuteilen. Der Betroffene stand im Verdacht, die Sozialhilfebehörden betrogen zu haben. Bei der Vernehmung hatte er erklärt, „vom Juni 1989 bis zum Februar 1990 im Bundesgebiet in verschiedenen Städten unterwegs gewesen zu sein". Die Anfrage wurde außerdem an den Verwaltungsausschuß des Landeswohlfahrtsverband Hessen (Hauptverwaltung) sowie nachrichtlich an sämtliche Regierungspräsidien des Landes Hessen gesandt, ebenfalls mit der Bitte, ggf. vorhandene Erkenntnisse über Sozialleistungen an den Betroffenen an das Polizeipräsidium weiterzuleiten.

Nicht nur die Anfrage bei sämtlichen Sozialministerien der Bundesländer, sondern auch die flächendeckende Abfrage innerhalb Hessens war unverhältnismäßig. Es hätte im einzelnen geklärt werden müssen, in welchem Gebiet sich der Beschuldigte konkret aufgehalten hat, um den Empfängerkreis einzugrenzen.

Die Bitte, eine Auflistung über alle Sozialhilfeleistungen zu übersenden, verstieß außerdem gegen § 73 Sozialgesetzbuch (SGB) X. Danach ist eine Offenbarung personenbezogener Daten zur Aufklärung eines Vergehens nur aufgrund einer richterlichen Anordnung zulässig. Diese lag hier jedoch nicht vor.

Auf meine förmliche Beanstandung teilte mir das Hessische Ministerium des Innern mit, die Staatsanwaltschaft Wiesbaden habe das Polizeipräsidium angewiesen, in geeigneter Weise Sozialämter zur Auskunftserteilung über evtl. weitere Sozialhilfegeldleistungen anzuschreiben. Eine konkretisierende Rückfrage bei dem Verdächtigen habe aus ermittlungstaktischen Gesichtspunkten nicht erfolgen können, da in diesem Fall der Betroffene unter Belehrung über sein Auskunftsverweigerungsrecht als Belasteter wohl nicht die gewünschten Angaben gemacht hätte.

Diese Bewertung überzeugt freilich nicht. Die Polizei ging lediglich aufgrund eines vagen Verdachts von einem über mehrere Bundesländer verteilten Aktivitätsbereich des Verdächtigen aus. Taktische Gründe können nicht zum Anlaß genommen werden, Ermittlungsersuchen entsprechend zu streuen, wenn weniger tief in die Rechte des Betroffenen eingreifende Maßnahmen möglich sind.

Zur Frage der fehlenden richterlichen Anordnung nahm das Ministerium keine Stellung, um nicht in ein schwebendes Verfahren einzugreifen. Dies ist kaum verständlich, da sich diese Anforderung durch einfaches Lesen des Gesetzestextes feststellen läßt.

7.3
Verbreitung von Informationen aus Homosexuellen-Publikationen durch Polizeidienststellen

7.3.1
Folgen eines Aufrufs

In einer Pressekonferenz hatte der Bundesverband Homosexualität zum Widerstand gegen Maßnahmen des bayerischen Innenministeriums zur Verhütung und Bekämpfung von AIDS aufgerufen. Daraufhin leitete die Staatsanwaltschaft Bonn gegen den Verband ein Ermittlungsverfahren wegen öffentlicher Aufforderung zu Straftaten (§ 111 Strafgesetzbuch) ein.

Im Rahmen des Ermittlungsverfahrens schickte das Landeskriminalamt in Düsseldorf an alle Landeskriminalämter „Erkenntnismitteilungen", in denen es um Auskunft bat, wo der Bundesverband Homosexualität seinen Sitz habe, und wer die Verantwortlichen dieses Verbandes seien.

Bei Nachforschungen im Polizeipräsidium in Frankfurt/M. stießen dort die Beamten auf eine vom Bundesverband Homosexualität Anfang 1987 herausgegebene Zeitschrift mit dem Titel „Nummer". Darin wurde über die Gründungsversammlung des Verbandes am 2. November 1986 in Köln berichtet. In einem Artikel wurde außerdem unter der Überschrift „Gegen den Zwangstest!" dazu aufgefordert, die Maßnahmen der bayerischen Gesundheitsbehörden im Zusammenhang mit der Bekämpfung der Immunschwächekrankheit AIDS nicht ohne weiteres hinzunehmen. Personen, die eine Vorladung zum HIV-Antikörpertest von den örtlichen Gesundheitsbehörden erhalten hatten, wurde geraten, hiergegen Widerspruch einzulegen. Zur Unterstützung dieser Kampagne druckte die Zeitschrift eine Musterwiderspruchserklärung ab.

Das Polizeipräsidium fertigte ein Fernschreiben, in dem leicht gekürzt der Wortlaut der ersten Seite dieser Ausgabe wiedergegeben, die Vorstandsmitglieder des neu gegründeten Bundesverbandes namentlich benannt und das Programm geschildert wurden. Als Quelle wurde die Zeitschrift zitiert. Schließlich wies das Polizeipräsidium darauf hin, daß in der Ausgabe Juli/August 1987 dieser Zeitschrift eine Reihe von Persönlichkeiten die Aktion des Bundesverbandes unterstützt hätten und nannte deren Namen. Dieses Fernschreiben schickte das Polizeipräsidium an das LKA in Wiesbaden, das Hessische Innenministerium (Lagezentrum), das Nordrhein-Westfälische

Innenministerium (Lagezentrum), das LKA in Düsseldorf, den Polizeipräsidenten in Bonn (14. Kommissariat) sowie das BKA in Meckenheim. Das Hessische Landeskriminalamt als Adressat dieses Fernschreibens fertigte wiederum ein Kopie an und sandte diese allen anderen Landeskriminalämtern sowie dem Landesamt für Verfassungsschutz in Wiesbaden zu.

Der Bundesverband Homosexualität erfuhr von der Archivierung dieser Zeitschrift sowie von der Weitergabe der Daten und wandte sich sowohl an den Bremer Datenschutzbeauftragten als auch an mich.

7.3.2
Datenverarbeitung der hessischen Polizeibehörden

Meine Überprüfung beim Polizeipräsidium in Frankfurt ergab, daß die Namen der in dem Fernschreiben bezeichneten Personen nicht in polizeilichen Unterlagen als Suchkriterien gespeichert waren, und zwar weder in automatisierten Dateien noch in automatisierten Karteien oder Akten. Allerdings wurde mir bestätigt, daß die Zeitschrift von Polizeibeamten in einem Homosexuellenlokal vorgefunden und mitgenommen worden war. Als Druckschrift wurde sie im Polizeipräsidium nicht personenbezogen abgelegt, sondern nach Aussagen der Beamten als Hintergrundmaterial für die Arbeit des „Sittenkommissariats" K 13 archiviert. Die Polizei wies darauf hin, daß dieses Kommissariat neben der Bearbeitung von Straftaten insbesondere daran interessiert sei, Homosexuelle auf die Gefahren durch Raubüberfälle durch männliche Prostituierte hinzuweisen. Eine aufgeschlossene, offene und auf Vertrauen zielende Zusammenarbeit auch mit den Homosexuellenverbänden sei deshalb für die Polizei von großer Bedeutung.

Als die Frankfurter Polizei 1987 die Zeitschrift „Nummer" aus dem Homosexuellenlokal mitnahm und aufbewahrte, gab es noch keine dem Volkszählungsurteil des Bundesverfassungsgerichts entsprechenden gesetzlichen Regelungen für die polizeiliche Datenverarbeitung. Bis zur Novellierung des HSOG am 1. Januar 1990 nahm die Polizei für ihre Tätigkeit den sogenannten „Übergangsbonus" in Anspruch. Aber auch die Datenverarbeitung, die für eine Übergangszeit aufgrund der allgemeinen polizeirechtlichen Vorschriften durchgeführt wurde, muß sich an der Verfassung messen lassen. Es können deshalb durchaus die neuen Verarbeitungsregelungen des HSOG zur Bewertung herangezogen werden, da sie die verfassungsrechtlichen Anforderungen an die polizeiliche Datenverarbeitung konkretisieren.

Nach den neuen Bestimmungen kann die Vollzugspolizei personenbezogene Daten zur Erfüllung ihrer Aufgaben erheben, wenn u.a. die Daten allgemein zugänglichen Quellen entnommen werden können (§ 44a Abs. 1 Nr. 3 HSOG). Die Polizei darf den Inhalt von Zeitschriften ohne weiteres im Rahmen von Strafermittlungsverfahren und zu Zwecken der Gefahrenabwehr unmittelbar weiterverwerten. Zum damaligen Zeitpunkt, als die Polizei die Zeitschrift „Nummer" mitnahm, geschah dies weder zur konkreten Strafermittlung noch zur unmittelbaren Gefahrenabwehr. Unzulässig wäre daher auf jeden Fall eine personenbezogene Auswertung und automatisierte Erfassung der in dem Artikel genannten Namen gewesen. Eine solche hat die Polizei aber, wie meine Prüfung ergeben hat, nicht vorgenommen. Damit stellt sich die Frage: Durfte der Artikel im Sachzusammenhang „Homosexualität" ohne unmittelbaren Personenbezug archiviert werden?

Zweifellos wird die Polizei in der Erhebungsphase, d.h. beim Lesen von Druckschriften auch mit personenbezogenen Informationen konfrontiert, die sie später im Rahmen der Weiterverwendung nicht benötigt. Solange das Material lediglich als „Hintergrundinformation" in einem allgemeinen Archiv oder der Bibliothek der Polizei abgelegt wird und nicht unmittelbar in die Strafermittlungen oder Maßnahmen der Gefahrenabwehr eingebracht wird, ist dagegen nichts einzuwenden. Keinesfalls darf jedoch durch eine unmittelbare Verknüpfung von Daten aus Druckschriften mit der Verwertung in den eigentlichen Informationssystemen, Dateien und Akten der Polizei eine getrennte, zweckgebundene Verwertung umgangen werden.

Unzulässig war jedoch die breitgestreute Übermittlung. Über die konkret ermittelnde und anfragende Dienststelle (LKA Düsseldorf) hinaus erhielt eine Vielzahl von Empfängern, die den Hintergrund lediglich umrissen oder – so das Hessische Landesamt für Verfassungsschutz – überhaupt nicht kannte, detaillierte personenbezogene Informationen, die als Belastung der Betroffenen interpretiert werden konnten. Dies gilt besonders für die Weiterversendung einer Kopie des Fernschreibens durch das Hessische Landeskriminalamt an alle anderen Landeskriminalämter und das Hessische Landesamt für Verfassungsschutz. Das Polizeipräsidium in Frankfurt durfte seine Erkenntnisse nur unmittelbar an die anfragende Stelle weiterleiten.

Das Hessische Ministerium des Innern hat mir mitgeteilt, daß es meine Rechtsansicht in allen Punkten teilt. Es hat daher das Hessische Landeskriminalamt und das Polizeipräsidium in Frankfurt angewiesen, in Zukunft bei ähnlichen Fällen lediglich die Behörden zu unterrichten, die die Daten zur Erfüllung ihrer Aufgaben benötigen.

7.4
Änderung des Anhörungs- und Vernehmungsbogens der Polizei

In mehreren Eingaben wurde ich auf ein von allen hessischen Polizeibehörden verwendetes Formular „Schriftliche Äußerung/Vernehmung von Beschuldigten/Betroffenen" aufmerksam gemacht. Der Vordruck – er wird verwandt, wenn jemandem eine Ordnungswidrigkeit oder eine Straftat vorgeworfen wird – enthielt mehrere datenschutzrechtliche Mängel:

Die Hinweise, bei welchen Fragen des Vordruckes eine Auskunftspflicht bestand und welche Fragen freiwillig beantwortet werden konnten, waren nur mühsam dem Kleingedruckten zu entnehmen. Einem Betroffenen, der beim Einparken ein anderes Fahrzeug beschädigt hatte, war nicht ersichtlich, weshalb er die Höhe seines Nettoeinkommens und das seiner Ehefrau angeben sollte. Um so weniger sahen die Betroffenen einen Grund, die Polizei über ihre Zahlungsverpflichtungen und die Anzahl der von ihnen unterhaltenen Kinder zu informieren. Noch weniger Verständnis fanden (erwachsene) Betroffene dafür, daß sie Angaben über ihre evtl. auch verstorbenen Eltern machen sollten.

Ich forderte deshalb das Innenministerium auf, den landeseinheitlichen Vordruck zu überarbeiten. Das neue Formular enthält einen deutlichen Hinweis, daß die Betroffenen zur Angabe ihrer Personalien verpflichtet sind, ein Verstoß gegen diese Verpflichtung nach § 111 des Ordnungswidrigkeitengesetzes mit einem Bußgeld bedroht ist und alle weiteren, über die Personalien hinausgehenden Angaben freiwillig sind. Die Frage nach den evtl. verstorbenen Eltern wird nicht mehr gestellt, bei der Frage nach dem Einkommen und den weiteren Angaben zu den wirtschaftlichen Verhältnissen wird erklärt, daß die von den Betroffenen gemachten Angaben bei einer evtl. festzusetzenden Geldbuße oder Geldstrafe berücksichtigt werden können.

Auch wenn die Neufassung des Formulars mehr als ein Jahr benötigte, wurden damit doch wichtige datenschutzrechtliche Verbesserungen erzielt.

7.5
Polizeiliche Vorgangsverwaltung und Kriminalakten

Im Rahmen von Kontrollen bei zwei hessischen Polizeipräsidien stellte ich fest, daß dort personenbezogene Informationen zu einzelnen Personen ungeachtet des völlig unterschiedlichen Zusammenhangs in einer Art „Personenakte" zusammengeführt worden waren. Dabei wurde nicht differenziert, ob die jeweiligen Informationen diese Personen als Verdächtige, Beschuldigte oder aber Zeugen betrafen, oder sogar von den Betroffenen selbst als Anzeigeerstatter geliefert worden waren.

Diese Praxis entsprach nicht den Bestimmungen des HSOG. Nach § 20 Abs. 8 HSOG können die Polizeibehörden „zur Vorgangsverwaltung oder zur befristeten Dokumentation vollzugspolizeilichen (behördlichen) Handelns personenbezogene Daten speichern und ausschließlich zu diesem Zweck sonst verwenden." Damit wird deutlich, daß diese „Vorgangsverwaltung" getrennt von den eigentlichen Kriminalakten geführt werden muß. Denn mit der Erschließung der Kriminalakten durch automatisierte Dateien nach „Verdächtigen bzw. Beschuldigten" wäre es unvereinbar, andere Informationen so zu verknüpfen, daß diese in den Kriminalakten auftauchen und auch deren Schicksal – etwa im Hinblick auf Löschungsfristen – teilen. Denn nur nach dem jeweiligen Sachzusammenhang ist der einzelne Vorgang zu bewerten. In einer Datei, die nach dem Namen von Beschuldigten geordnet ist, haben die Namen von Anzeigeerstattern nur eine Hilfsfunktion und bilden kein „Erschließungskriterium", um den einzelnen Vorgang zu finden. An diesen Kriterien muß festgehalten werden, andernfalls wären ungerechtfertigte Belastungen für Einzelpersonen nicht auszuschließen.

Bisher hat das Hessische Ministerium des Innern keine internen Anweisungen erlassen, die eine solche getrennte Aktenführung gewährleisten. Nach dem Inkrafttreten des neuen HSOG sind solche Vorschriften jedoch unabdingbar. Die vorhandenen Unterlagen der Polizei müssen Schritt für Schritt durchforstet und entsprechend getrennt werden.

8. Gesetz über das Landesamt für Verfassungsschutz

In den letzten Tätigkeitsberichten habe ich immer wieder eine gesetzliche Grundlage für die Datenverarbeitung des Hessischen Landesamts für Verfassungsschutz angemahnt.

Am 19. Dezember 1990 hat der Gesetzgeber endlich das Gesetz über das Landesamt für Verfassungsschutz (GVBl. I S. 753) verabschiedet. Es ist bis auf die Bestimmungen über die parlamentarische Kontrolle der Tätigkeit des Landesamtes für Verfassungsschutz am 29. Dezember 1990 in Kraft getreten. Die Kontrollvorschriften gelten erst ab dem 5. April 1991.

Der Verabschiedung sind intensive Beratungen in den beteiligten Landtagsausschüssen vorausgegangen. Die Landesregierung hatte im Mai 1990 einen Gesetzentwurf im Landtag eingebracht (Drucks. 12/6582). Am 29. August führte der Innenausschuß dazu eine Anhörung von Sachverständigen durch. Als Konsequenz aus der Anhörung stellten sowohl die Fraktion der SPD (Drucks. 12/7511) als auch die Koalitionsfraktionen CDU und FDP (Drucks. 12/7590) umfassende Änderungsanträge zu dem Regierungsentwurf.

Der von der Landesregierung eingebrachte Entwurf hat im Laufe der parlamentarischen Beratungen, an denen ich mich durch Stellungnahmen beteiligt habe, aus datenschutzrechtlicher Sicht weitgehende Verbesserungen erfahren. Auch wenn es zu keiner Neubestimmung der Aufgaben des Verfassungsschutzes gekommen ist, obwohl dies wegen der politischen Veränderungen im Ost-West-Verhältnis dringend notwendig gewesen wäre, ist das verabschiedete Gesetz ein wichtiger Beitrag für eine den verfassungsrechtlichen Vorgaben entsprechende Regelung der Datenverarbeitung des Hessischen Landesamtes für Verfassungsschutz. Das hessische Gesetz ist deutlich besser als

das jüngst verabschiedete Bundesverfassungsschutzgesetz und die Gesetzentwürfe verschiedener Länder. Dennoch weist es eine Reihe von Defiziten auf.

8.1
Systematischer Ausgangspunkt

Das Gesetz über das Landesamt für Verfassungsschutz berücksichtigt nicht in ausreichendem Maße, daß den verschiedenen Aufgaben des Verfassungsschutzes wie Abwehr des politischen Extremismus, der Spionagebekämpfung oder der Mitwirkung bei Sicherheitsüberprüfungen jeweils unterschiedliche Befugnisse zugeordnet werden müssen. Es hätte nahegelegen, für jeden Aufgabenbereich gesondert die Datenverarbeitung zu regeln. Dadurch wäre ein Zwang entstanden, für jede einzelne Aufgabe des Verfassungsschutzes die notwendigen Befugnisse zu begründen. Augenfällig wird dies etwa beim Einsatz von nachrichtendienstlichen Mitteln: Während z.B. bei der Spionageabwehr der Einsatz solcher Mittel geboten sein kann, stellt sich die Situation im politischen, nicht konspirativ agierenden Extremismus anders dar. Aber auch bei anderen Formen der Informationserhebung z.B. bei der Einsicht des Landesamtes für Verfassungsschutz in von öffentlichen Stellen geführte Register wie beispielsweise das Personalausweis- oder Paßregister, die Führerschein- oder Waffenscheinkartei, wäre eine Differenzierung nach der jeweilig verfolgten Aufgabe erforderlich. Dies gilt auch für die Mitteilungspflichten und -befugnisse verschiedener öffentlicher Stellen an das Verfassungsschutzamt, die aufgabenspezifisch ausgestaltet werden sollten. Für die Regelung der zweckgebundenen Verwendung von Informationen über die je nach Aufgabenbereich unterschiedlichen Löschungsbestimmungen bis hin zu einer differenzierenden Ausgestaltung des Auskunftsrechts wäre eine derartige Systematik von Vorteil gewesen.

Das Gesetz bleibt dagegen auf der einen Seite bei der Bestimmung der Aufgaben, auf der anderen Seite bei der Festlegung der Befugnisse des Verfassungsschutzes, ohne daß bei diesen im erforderlichen Maße differenziert wird.

8.2
Aufgabenbeschreibung

Bei der Regelung der Aufgaben übernimmt das hessische Verfassungsschutzgesetz die aus dem Bundesgesetz und den Entwürfen anderer Bundesländer bekannten, wenig konkreten Umschreibungen. Zwar werden in Anlehnung an das Bundesverfassungsschutzgesetz z.B. derart vage Begriffe wie den der „Bestrebung gegen den Bestand des Bundes oder eines Landes" oder den der „Bestrebung, die gegen die freiheitlich demokratische Grundordnung gerichtet ist", näher erläutert, dabei wird aber nur auf weitere wenig aussagekräftige Formulierungen zurückgegriffen. Dem Bürger ist kaum geholfen, wenn er erfährt, daß der Verfassungsschutz Bestrebungen beobachtet, „die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden" (§ 2 Abs. 2 Nr. 3). Hier kommt hinzu, daß der Gewaltbegriff von der Rechtsprechung zum Teil sehr weit ausgelegt wird und deshalb schon beispielsweise Verkehrsblockaden oder Vorlesungsstörungen darunter subsumiert werden könnten.

Positiv zu bewerten ist allerdings die Klarstellung im Gesetz, daß es bei den vom Verfassungsschutz zu beobachtenden Bestrebungen in der Regel um entsprechende Verhaltensweisen in organisierten Personenzusammenschlüssen und nur im Ausnahmefall – unter einschränkenden Voraussetzungen – um solche von Einzelpersonen geht (§ 2 Abs. 3). Damit wurde meine Forderung, aus dem Grund der Verhältnismäßigkeit auf die Beobachtung von Einzelpersonen gänzlich zu verzichten, wenigstens ansatzweise berücksichtigt.

Für die vorgesehene Mitwirkung des Verfassungsschutzes bei Sicherheitsüberprüfungen (§ 2 Abs. 5 Nr. 1 und 2) fehlt es an der Festlegung, daß für die Durchführung einer derartigen Überprüfung eine eigenständige bereichsspezifische Rechtsgrundlage zu schaffen ist. In dieser wäre beispielsweise zu regeln, wer unter welchen Voraussetzungen einer derartigen Überprüfung unterzogen werden darf, wer für die Durchführung der Überprüfung zuständig ist und welche Informationseingriffe in diesem Zusammenhang erlaubt sein sollen. Die Schaffung entsprechender gesetzlicher Vorgaben ist gerade in Hessen besonders dringlich, da die derzeit geltenden „Richtlinien für die Sicherheitsüberprüfung von Landesbediensteten" aus dem Jahre 1962 – auch abgesehen von der mangelnden Gesetzesqualität – die Voraussetzungen und Modalitäten der Sicherheitsüberprüfung nur unzulänglich regeln.

8.3
Befugnisregelung

Die im Regierungsentwurf dem Landesamt für Verfassungsschutz eingeräumten Befugnisse sind im Laufe der parlamentarischen Beratungen zum Teil stark geändert worden.

8.3.1
Erhebung von Daten über „Verdächtige" und „Unbeteiligte"

Der Regierungsentwurf vom Mai 1990 enthielt noch eine allgemeine Befugnisnorm, nach der das Landesamt für Verfassungsschutz Informationen erheben durfte, auch wenn tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen oder sicherheitsgefährdende Tätigkeiten (noch) nicht vorlagen. Wäre es bei dieser Regelung geblieben, hätte das Landesamt für Verfassungsschutz beispielsweise Daten über Bürger sammeln können allein mit dem

Argument, es müsse prüfen, ob es sich um Teilnehmer einer verfassungsfeindlichen Bestrebung handelt. Das verabschiedete Gesetz berücksichtigt meine Kritik weitgehend, indem es festlegt, daß der Verfassungsschutz in den Fällen, in denen beispielsweise noch kein Verdacht für eine verfassungsfeindliche Bestrebung besteht, ausschließlich allgemein zugängliche Quellen und keine anderen Mittel zur Informationsgewinnung nutzen darf (§ 4 Abs. 1). Außerdem wird klargestellt, daß unter diesen Voraussetzungen beispielsweise öffentlichen Publikationen entnommene Informationen über eine Person erst dann in einer Datei oder in einer zur Person geführten Akte gespeichert werden dürfen, wenn sich entsprechende Verdachtsmomente ergeben haben (§ 6 Abs. 4). Beschränkt wurde außerdem die Möglichkeit, Informationen über sogenannte „Unbeteiligte" zu sammeln. § 3 Abs. 1 läßt dies nur in einigen wenigen, aus Sicht des Verfassungsschutzes unbedingt erforderlichen Fällen zu und legt präzise Löschungspflichten bzw. Verwertungsverbote fest. Der vom hessischen Gesetzgeber beschrittene Weg, konkret festzulegen, unter welchen einschränkenden Voraussetzungen Daten über Personen erhoben werden dürfen, bei denen keine Verdachtsmomente bestehen, ist eindeutig die bessere Lösung gegenüber einer Gesetzeslage, in der dies mehr oder weniger offen bleibt.

8.3.2
Akten- und Registereinsichtsrecht

Zu weitgehend ist das generelle Akten- und Registereinsichtsrecht für den Verfassungsschutz (§ 4 Abs. 2 Satz 2). Anders als beim Auskunftsrecht führen diese Befugnisse in der Regel dazu, daß weit mehr Informationen gewonnen werden als für die Aufgabenerfüllung erforderlich sind. Deshalb dürfen derartige Einsichtsrechte dem Verfassungsschutz allenfalls als spezielle Erhebungsmethoden in eng begrenzten Ausnahmefällen zur Verfügung stehen. Es fehlt aber im Gesetz an einer präzisen Festlegung, in welche Register der Verfassungsschutz unter welchen Voraussetzungen einsehen darf.

8.3.3
Einsatz nachrichtendienstlicher Mittel

Das Gesetz regelt nicht, welche nachrichtendienstlichen Mittel wie z.B. der Einsatz von V-Leuten, Observationen, Bild-und Tonaufzeichnungen das Landesamt für Verfassungsschutz anwenden darf, sondern überläßt die Festlegung einer Dienstvorschrift (§ 3 Abs. 2). Immerhin muß aber die Dienstvorschrift der parlamentarischen Kontrollkommission übersandt werden (§ 3 Abs. 2 Satz 3).

Bei der Regelung des Einsatzes nachrichtendienstlicher Mittel wirkt sich die vom Gesetzentwurf angestrebte Differenzierung zwischen der Erhebung von Informationen „Verdächtiger" und „Unbeteiligter" positiv aus. Meine Forderung, daß nachrichtendienstliche Mittel nur gegen konkret Verdächtige, nicht aber gegen Dritte, die keinen Anlaß zur Beobachtung gegeben haben, angewandt werden dürfen, wurde insoweit aufgegriffen, als ein gezielter Einsatz gegenüber Unbeteiligten in diesen Fällen ausgeschlossen wird (§ 5 Abs. 3). Werden z.B. beim auf eine bestimmte verdächtige Person zielenden Einsatz einer Videokamera auch Aufnahmen von Unbeteiligten festgehalten, sind diese unverzüglich zu löschen (§ 5 Abs. 3 i.V.m. § 3 Abs. 1 Satz 3).

8.4
Zeitliche Begrenzung der Datenspeicherung

Meine beim Landesamt für Verfassungsschutz im Jahre 1989 durchgeführte Prüfung hatte gezeigt, daß die zeitlich beschränkte Speicherung ein wichtiges Instrument ist, um die Informationssammlung des Verfassungsschutzes auf das erforderliche Maß zu begrenzen (vgl. 18. Tätigkeitsbericht, Ziff. 5.1.6). Erforderlich sind deshalb detaillierte gesetzliche Vorgaben, die den Verfassungsschutz verpflichten, die Aufbewahrung von Informationen nach festgesetzten Fristen zu überprüfen, und in den Fällen, in denen eine Prüfung nicht erfolgt, die Informationen zu vernichten.

Das Gesetz verpflichtet das Landesamt für Verfassungsschutz nach von ihm festzusetzenden Fristen, spätestens aber nach 5 Jahren, eine entsprechende Überprüfung vorzunehmen. Darüber hinaus sind bestimmte Informationen grundsätzlich nach 10 Jahren zu sperren und dürfen damit nicht weiter verwendet werden (§ 6 Abs. 6). Damit bleibt das Gesetz hinter meiner Forderung zurück. Die Praxis der nächsten Jahre wird zeigen, ob die Regelungen ausreichen.

8.5
Datenaustausch zwischen dem Landesamt für Verfassungsschutz und anderen Behörden

Die Bestimmungen, die einen Datenaustausch zwischen dem Landesamt für Verfassungsschutz und anderen öffentlichen Stellen vorsehen, gehen sehr weit. Dabei ist zu berücksichtigen, daß sich aus dem Gebot der Trennung von Polizeibehörden einerseits und Geheimdiensten andererseits über die organisationsrechtlichen Anforderungen hinaus weiterreichende Konsequenzen für den Informationsaustausch zwischen diesen Behörden ergeben. Da das Trennungsgebot über die Verfassungsgebote der Verhältnismäßigkeit und Zweckbindung konkretisiert wird, muß der Gesetzgeber entsprechende Einschränkungen für den Informationsverbund vorsehen.

Unvereinbar mit dem Trennungsgebot wäre der in früheren Entwürfen unter bestimmten Voraussetzungen zugelassene automatisierte Zugriff potentiell aller hessischen Behörden, insbesondere der Polizeibehörden, auf

Dateien des Landesamtes für Verfassungsschutz. Die Landesregierung hatte aufgrund der massiven Kritik in ihrem Entwurf deshalb darauf verzichtet. Allerdings hätten einige der vorgesehenen traditionellen Übermittlungsbefugnisse auch einer Einschränkung bedurft. So dürfen unterschiedslos alle hessischen öffentlichen Stellen dem Landesamt für Verfassungsschutz Daten übermitteln, wenn nach ihrer Einschätzung die Informationen für die Aufgabenerfüllung des Landesamtes erforderlich sind (§ 8 Abs. 1). Meine Forderung, diese Spontanübermittlungen in Anlehnung an die entsprechende Regelung des Bundesverfassungsschutzgesetzes auf Informationen aus dem gewaltorientierten Extremismus und der Spionage zu beschränken, wurde nicht berücksichtigt.

Darüber hinaus sind Polizeibehörden nach § 8 Abs. 2 verpflichtet, alle personenbezogenen Daten zu übermitteln, die sie für die Aufgabenerfüllung des Verfassungsschutzes erforderlich halten. Auch hier wurde mein Vorschlag, die Übermittlung auf solche Informationen zu beschränken, die im Zusammenhang mit der Ermittlung von Staatsschutzdelikten entstehen, nicht akzeptiert.

Ähnliches gilt für die Regelung der Datenübermittlung des Verfassungsschutzes an andere Behörden. Wenn wie in § 10 bei der Weitergabe von Informationen an die Strafverfolgungsbehörden nicht nur auf Staatsschutzdelikte, sondern auch auf „sonstige Straftaten, bei denen aufgrund ihrer Zielsetzung, des Motivs des Tatverdächtigen oder dessen Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, daß sie gegen die in Artikel 73 Nr. 10 Buchstabe b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind", abgestellt wird, ist dies äußerst bedenklich. Nach meinen Erfahrungen mit der beim BKA geführten „Arbeitsdatei PIOS Innere Sicherheit (APIS)" besteht bei einer derartigen Formulierung die Gefahr, daß auch bei einem relativ oberflächlichen politischen Bezug Datenübermittlungen an die Polizei zu erwarten sind.

8.6
Auskunftsregelung

Die Regelung des Anspruchs des Bürgers auf Auskunft über die zu seiner Person beim Landesamt für Verfassungsschutz gesammelten Informationen (§ 18) ist insgesamt im Vergleich zu entsprechenden anderen Vorschriften auf Bundes- oder Landesebene positiv zu bewerten.

Zwar wäre in diesem Bereich eine nach den Aufgaben des Verfassungsschutzes differenzierende Betrachtung ganz besonders wichtig gewesen. Denn was z.B. im Spionagebereich mit guten Gründen geheimgehalten wird, kann im Rahmen der Sicherheitsüberprüfung möglicherweise ohne weiteres dem Betroffenen mitgeteilt werden. Auch hier hat sich der Gesetzgeber aber gegen eine auf die verschiedenen Sachverhalte abgestimmte Regelung entschieden.

Die Auskunftsbestimmung lehnt sich weitgehend an die bisher auch für den Verfassungsschutz geltende Regelung im Hessischen Datenschutzgesetz an. Danach besteht ein Anspruch des Bürgers darauf, daß der Verfassungsschutz in jedem Einzelfall eine Abwägung vorzunehmen hat zwischen dem Auskunftsrecht des einzelnen und dem öffentlichen Interesse oder Interessen Dritter an der Geheimhaltung. Neu hinzugekommen ist eine abschließende Festlegung derjenigen Sachverhalte, in denen ein derartiges Geheimhaltungsinteresse vorliegen soll. Da die entsprechenden Formulierungen teilweise wenig präzise sind, ist abzuwarten, ob damit ein Stück mehr Transparenz für den Betroffenen erreicht wird.

9. Justiz

9.1
Der „gläserne" Staatsanwalt

Ein Sonderdezernat der Staatsanwaltschaft beim Oberlandesgericht Frankfurt führt seit einiger Zeit eine automatisierte Datei, in der sämtliche in Hessen auf dem Gebiet des Umweltschutzes anhängigen Ermittlungs- und Strafverfahren erfaßt werden. Die für die Verfolgung von Umweltstraftaten zuständigen Staatsanwälte bei den Landgerichten sind gem. einer Rundverfügung des Hessischen Justizministeriums vom 15. November 1988 verpflichtet, dem Sonderdezernenten beim OLG, der die Dienst- und Fachaufsicht über sie ausübt, auf einem festgelegten Formular die bei ihnen anhängigen Verfahren mitzuteilen. Jährlich erfolgen etwa 3000 Meldungen. Neben Angaben wie Name und Vorname des Beschuldigten, des Tatorts und die Bezeichnung der Straftat, die Art der Erledigung (Anklage oder Einstellung des Verfahrens in jeweils verschiedenen Varianten) ist auf dem Meldeformular auch ausdrücklich die Kennziffer des Dezernenten, d.h. des einzelnen Staatsanwalts bei den Landgerichten aufgeführt.

Diese automatisierte Datei bietet eine Vielzahl von Auswertungsmöglichkeiten. Aus ihr läßt sich ein genaues Abbild der von den einzelnen Staatsanwälten durchgeführten Verfahren herstellen. Sie liefert nicht nur eine Erledigungsstatistik über alle in einem bestimmten Jahrgang abgeschlossenen Fälle mit der konkreten Art der Erledigung, sondern über weitere Suchprogramme auch Erkenntnisse über die Art der einzelnen Straftaten.

Unbehagen bei den Staatsanwälten verursachte jedoch, daß genau festgestellt werden könnte, welches Dezernat wie viele Fälle in welchem Zeitraum und mit welchem Ergebnis abgeschlossen hat. Die mit der Dienst- und Fachaufsicht betraute Staatsanwaltschaft bei dem Oberlandesgericht wäre demnach in der Lage, jederzeit genau die Leistung des

einzelnen Staatsanwalts zu überprüfen. Einzelne Staatsanwälte äußerten daher mir gegenüber die Besorgnis, die an die Aufsichtsbehörde weitergeleiteten Daten könnten bei Personalentscheidungen wie z.B. Beförderungen genutzt werden.

Die Staatsanwaltschaft bei dem OLG versicherte mir allerdings, daß sie die Daten an keine weitere Dienststelle weiterleite, da die befürchteten Auswertungen auch allenfalls vor dem Hintergrund der Kenntnis von regionalen Besonderheiten aussagefähig wären: Die Statistik erlaube nur in begrenztem Umfang Aussagen über das Leistungsvermögen der einzelnen Staatsanwälte. So habe etwa die Einführung eines Geländewagens bei einer Polizeistation in einem Jahr dazu geführt, daß die Polizeibeamten eine Vielzahl von Landwirten anzeigten, auf deren Feldern nicht untergegrabene Jauche aufgebracht worden war. Alle diese Fälle mußte die Staatsanwaltschaft bearbeiten. Die Statistik kletterte aus diesem Grund in die Höhe, ohne daß dies etwa als Argument für eine mangelnde Ermittlungstätigkeit in anderen Bezirken hätte herangezogen werden können. In einem anderen Fall hatte die Übersendung einer Liste von sogenannten Kleineinleitern (von flüssigem Abfall in Oberflächengewässer) durch einen Anzeigenerstatter an die Staatsanwaltschaft eine ebenso hohe Zunahme der Strafverfahren zur Folge. Allerdings wurden alle Verfahren später wieder eingestellt.

Auch wenn kein Zweifel besteht, daß eine automatisierte Aufbereitung des Zahlenmaterials zur Durchführung der Fach- und Dienstaufsicht „erforderlich" im Sinne des Hessischen Datenschutzgesetzes und damit zulässig ist, ist der Fragebogen doch korrekturbedürftig. Es dürfte für Zwecke der Fach- und Dienstaufsicht genügen, die Statistik ohne eine Aufschlüsselung bis zur Ebene der einzelnen Dezernate bei den Staatsanwaltschaften, und damit bis zu den Staatsanwälten selbst, zu führen. Auch so kann die Übersichts- und Leitungsfunktion durch die Staatsanwaltschaft bei dem OLG wirksam ausgeübt werden.

Ein absolutes Verbot, bei Personalentscheidungen auf Daten aus der Datei zurückzugreifen, ist aus den gesetzlichen Bestimmungen kaum ableitbar. In jedem Fall ist es jedoch notwendig, die Problematik der auf diese Weise gewonnenen Zahlen zu berücksichtigen und keinerlei Aussagen zu treffen, die etwa aufgrund der besonderen Umstände einzelner Meldungen nicht eindeutig begründet werden können. Selbst wenn eine solche „Aufsichtsdatei" nicht als „automatisierte Verarbeitung von Daten von Beschäftigten" im Sinne von § 34 Abs. 5 des Hessischen Datenschutzgesetzes zu bewerten ist, da im Vordergrund nicht die Entscheidung über das Personal, sondern die Dienst- und Fachaufsicht steht, so ist der in § 34 Abs. 1 verankerte Erforderlichkeitsgrundsatz – der im übrigen das gesamte Datenschutzrecht beherrscht – strikt zu beachten.

Ich habe das Hessische Justizministerium auf das Problem hingewiesen. Eine Stellungnahme des Ministeriums steht noch aus.

9.2
Prozeßkostenhilfe

Ein Bürger beschwerte sich bei mir darüber, daß in einem gerichtlichen Verfahren zusammen mit den übrigen Akten auch seine Prozeßkostenhilfeakten aus einem anderen Gerichtsverfahren beigezogen worden waren.

Verfügt eine Partei im Zivilprozeß nicht über die nötigen Mittel, um ihre Rechtsverfolgung oder Rechtsverteidigung bestreiten zu können, so wird ihr unter bestimmten Voraussetzungen nach den Bestimmungen der ZPO eine Prozeßkostenhilfe oder ein Prozeßkostenvorschuß gewährt.

Um diese Unterstützung zu erhalten, muß der Betroffene allerdings dem Gericht eine Erklärung über seine persönlichen und wirtschaftlichen Verhältnisse (Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten) einschließlich der entsprechenden Belege vorlegen.

Unter anderem zum Schutz des Rechts auf informationelle Selbstbestimmung des Betroffenen enthalten die Durchführungsbestimmungen der Landesjustizverwaltungen und des Bundesministers der Justiz zum Gesetz über die Prozeßkostenhilfe vom 1. Oktober 1985 Vorschriften, nach denen die ausgefüllten Vordrucke mit den Erklärungen über die persönlichen und wirtschaftlichen Verhältnisse sowie die bei der Durchführung der Prozeßkostenhilfe entstehenden Vorgänge in allen Fällen und für jeden Beteiligten in einem besonderen Beiheft zu vereinigen sind. In das Beiheft sind auch Durchschriften der die Prozeßkostenhilfe betreffenden gerichtlichen Entscheidungen zu nehmen.

Ich habe das Gericht darauf hingewiesen, daß die Versendung der Akten über die Prozeßkostenhilfe unzulässig war, da die Einrichtung des Beiheftes ja gerade bewirken soll, daß Dritte von den darin enthaltenen Vorgängen nur Kenntnis erhalten, wenn dies unabdingbar ist. Das Gericht teilte mir mit, es habe sich um ein Versehen gehandelt.

Dann wies mich der Betroffene darauf hin, daß auch in der Hauptakte detaillierte Angaben über seine persönlichen und wirtschaftlichen Verhältnisse enthalten seien.

Dies traf in der Tat zu. Der Grund war folgender: Das Landgericht hatte den Antrag des Betroffenen auf Gewährung von Prozeßkostenhilfe in erster Instanz abgelehnt. Seine Beschwerde hatte keinen Erfolg. Das Oberlandesgericht Frankfurt bestätigte die Entscheidung des Landgerichts. Sowohl der Beschluß des Landgerichts als auch des

Oberlandesgerichts enthielten detaillierte Angaben zu den Vermögensverhältnissen des Betroffenen. Während noch der ursprüngliche ablehnende Beschluß, ebenso wie im übrigen allgemein positive Beschlüsse zugunsten des Antragstellers, keine detaillierten Angaben zu den wirtschaftlichen Verhältnissen enthielten, mußte in den nachfolgenden Entscheidungen der Gerichte für den Beschwerdeführer schlüssig und nachvollziehbar im einzelnen dargelegt werden, warum seinen Rechtsmitteln nicht entsprochen werden konnte. Ohne detaillierte Angaben, auch zu seiner persönlichen und Vermögenssituation, war dies nicht möglich. Die erwähnten Durchführungsbestimmungen verlangen, daß die Beschlüsse insgesamt, d.h. auch mit den Begründungen, in der Hauptakte abzuheften sind. Zwar werden auch in das Beiheft Durchschriften der gerichtlichen Entscheidungen aufgenommen. Die mit dem Beiheft beabsichtigte Trennung der Informationen vom Hauptverfahren ist jedoch damit faktisch aufgehoben.

Ich habe das Hessische Justizministerium aufgefordert, eine Änderung der Durchführungsbestimmungen zu prüfen. In die Hauptakte könnte lediglich der Entscheidungstenor aufgenommen und die Begründung in der Beiakte belassen werden.

10. Meldebehörden: Übermittlung an öffentlich-rechtliche Stellen zu fiskalischen Zwecken

Anfang 1990 erhielt eine Reihe von Gemeinden eine Anfrage einer Generalvertretung der Deutschen Bundesbahn. Die Generalvertretung bat um Übersendung der Anschriften aller Einwohner, die im Jahre 1990 das 60. Lebensjahr vollendeten; sie beabsichtigte, die Betroffenen in einem persönlichen Anschreiben über die Vorteile eines Seniorenpasses zu informieren.

Kurz nach einem Wohnungswechsel erhielt ein Einwohner einer südhessischen Stadt einen „Begrüßungsbrief" der ortsansässigen öffentlich-rechtlichen Sparkasse. Sie bot die Anknüpfung von Geschäftsverbindungen sowie ihren Service an. Die Sparkasse hatte die Anschrift von der Meldebehörde erhalten, die sie regelmäßig über alle neu zugezogenen Einwohner informierte.

Eine Stadt im Rhein-Main-Gebiet hatte einer öffentlich-rechtlichen Stiftung die Anschriften aller erwachsenen Einwohner zur Durchführung einer Spendensammlung zur Verfügung gestellt. Zweck der Stiftung ist, den Einwohnern der Stadt in Notfällen soziale Hilfestellungen zu geben.

In allen drei Fällen waren die Empfänger zwar öffentlich-rechtliche Einrichtungen, dennoch konnte die Übermittlung der Meldedaten hier nicht auf § 31 Hessisches Meldegesetz gestützt werden, der die Weitergabe von Meldedaten an öffentliche Stellen privilegiert.

Auch wenn die Bundesbahn ein öffentlich-rechtliches Unternehmen ist, bei ihrer Öffentlichkeitsarbeit handelt sie dort, wo sie im Wettbewerb mit privaten Verkehrsbetrieben eine mit der Wirtschaft vergleichbare Werbung betreibt nicht öffentlich-rechtlich, sondern fiskalisch (vgl. BVerfGE 47, 274, 250). Die Werbekampagne, mit der die über 60jährigen von den Vorzügen eines Seniorenpasses überzeugt werden sollten, erfolgte nicht im Rahmen der öffentlichen Aufgabenerfüllung der Deutschen Bundesbahn.

Auch soweit Sparkassen Stellen des öffentlichen Rechts sind und § 2 des Hessischen Sparkassengesetzes ihnen eine allgemeine öffentlich-rechtliche Aufgabenerfüllung zuweist, wäre es mit dem Gleichheitssatz des Art. 3 Abs. 1 I Grundgesetz nicht vereinbar, sie bei der Erteilung von Melderegisterauskünften gegenüber privaten Banken zu bevorzugen. Sparkassen können sich daher bei der Bitte um Auskünfte aus dem Melderegister nicht wirksam auf ihre öffentlich-rechtliche Aufgabenstellung berufen.

Gleiches galt für die Stiftung: Zwar sind Stiftungen des öffentlichen Rechts auch Verwaltungsträger. Im Vordergrund der Erfüllung eines Stifungszweckes steht aber immer eine Vermögensmasse, deren Ertrag einem bestimmten Zweck zugute kommen soll. Nur im Zusammenhang mit der Wahrnehmung dieser Aufgabe kann sich eine Stiftung auf ihre öffentlich-rechtliche Aufgabenerfüllung stützen. Die Spendensammlung diente jedoch nicht der Verteilung des Ertrages aus der Vermögensmasse, sondern der Ansammlung zusätzlichen Kapitals und war somit ebenfalls keine öffentlich-rechtliche Aufgabenerfüllung.

Die Empfänger hatten unter wirtschaftlichen Gesichtspunkten sicherlich ein legitimes Interesse, die Meldedaten zu erfahren. Regelungsgegenstand des § 31 Abs. 1 ist aber die Privilegierung der hoheitlichen staatlichen Eingriffs- oder Leistungsverwaltung öffentlicher Stellen. Die Daten sollten aber gerade nicht für diese Zwecke verwendet werden. Die gewünschten Datenübermittlungen mußten deshalb die Zulässigkeitsvoraussetzungen für die Weitergabe von Meldedaten an private Dritte erfüllen (§ 34 Hessisches Meldegesetz). Da es sich jeweils um eine Vielzahl von den Anfragern nicht namentlich bezeichneter Einwohner handelte, mußte für die Übermittlungen ein öffentliches Interesse bestehen (§ 34 Abs. 3).

Das öffentliche Interesse ist nicht deckungsgleich mit „Allgemeinwohl" oder „Gemeinnützigkeit". Auch allgemeinunterstützenswerte kulturelle, sportliche oder gesellschaftliche Aktivitäten genügen nicht, um ein öffentliches Interesse zu begründen. Es müssen vielmehr Belange der Allgemeinheit betroffen sein, z.B. wissenschaftliche Forschungszwecke, gesamtwirtschaftliche Planungen oder karitative Zwecke sowie Aktionen der Gesundheitsvorsorge.

Die Melderegisterauskünfte an die Deutsche Bundesbahn und die Sparkasse lagen nicht im öffentlichen Interesse. Hier stand das kommerzielle Interesse der Auskunftsuchenden zu sehr im Vordergrund. Dagegen war bei der Spendenaktion der Stiftung die Nähe zur Tätigkeit anderer öffentlicher Stellen, nämlich der Sozialleistungsträger, deutlich sichtbar. Die Entscheidung des Gemeindevorstands, der in diesem Fall ein öffentliches Interesse an der Auskunft bejahte, war daher nicht ermessensfehlerhaft.

11. Kommunen: Ratsinformationssysteme

11.1
Funktion und Modellprojekte

„Ratsinformationssysteme" (RIS) – so der für das Projekt der Stadt Kassel verwendete Begriff – dienen dem Ziel, mit den Mitteln der automatisierten Datenverarbeitung (ADV) die Arbeitsmöglichkeiten der Gemeindevertreter bzw. der Fraktionen in den Gemeindeparlamenten zu verbessern. Erleichtert werden soll vor allem der Zugriff auf die für die parlamentarische Arbeit relevanten Magistratsbeschlüsse und auf die Dokumente der Gemeindevertretung selbst. Dies reicht von den Tagesordnungen für die Plenar- und Ausschußsitzungen über die Vorlagen des Gemeindevorstands/Magistrats bis hin zu den Niederschriften und Protokollen.

In Hessen am weitesten entwickelt ist nach meiner Kenntnis das Ratsinformationssystem (RIS) der Stadt Kassel. An der Vorbereitung war ich intensiv beteiligt. Das Verfahren „Kommunaler Sitzungsdienst" der Stadt Wiesbaden steckt dagegen noch in den Anfängen. Hier geht es zunächst nur um den Zugriff der städtischen Parlamentarier auf den Betreff, die jeweiligen Suchbegriffe und die Vorlagen bzw. Beschlüsse des Magistrats und der Stadtverordnetenversammlung. Die Protokolle sollen erst in künftigen Ausbaustufen des Projekts gespeichert werden.

Zu meinen gesetzlichen Aufgaben gehört nicht nur die Überwachung der Einhaltung der Datenschutzvorschriften. Nach § 24 Abs. 2 HDSG hat der Hessische Datenschutzbeauftragte auch darauf zu achten, ob die ADV zu einer Verschiebung in der Gewaltenteilung zwischen den Organen der kommunalen Selbstverwaltung führt, und ggf. geeignete Gegenmaßnahmen anzuregen. Zweifellos kann ein effizientes automatisiertes Ratsinformationssystem Wissens- und damit Einflußverluste zu Lasten der „kommunalen Legislative" vermindern helfen und ist in diesem Kontext prinzipiell positiv zu bewerten.

11.2
Die Hessische Gemeindeordnung als Zugriffsrahmen

Auf der anderen Seite – und dies hat sich als wohl entscheidendes Problem bei der konkreten Ausgestaltung der „Ratsinformationssysteme" herausgeschält – dürfen die von der Hessischen Gemeindeordnung (HGO) vorgesehenen Informationszuteilungen und Mitteilungsflüsse nicht durch die Automation des Datenzugangs verändert oder erweitert werden. Steht nach der HGO eine bestimmte Unterlage in Papierform nur einer bestimmten Personengruppe zur Verfügung, muß die parallele Zugriffsbeschränkung auch im automatisierten Ratsinformationssystem sichergestellt werden.

Bestes Beispiel für diese Aussage ist § 50 Abs. 2 Satz 4 HGO: Nach dieser Vorschrift kann die Gemeindevertretung/Stadtverordnetenversammlung beschließen, daß der Gemeindevorstand Niederschriften über das Ergebnis seiner Sitzung an die Vorsitzenden der Gemeindevertretung bzw. der Fraktionen weiterzugeben hat. Der Umkehrschluß ergibt, daß die Protokolle der Magistratssitzungen nicht an alle Stadtverordneten weitergegeben werden dürfen. Selbstverständlich muß diese gesetzliche Begrenzung der Zugangsberechtigungen in einem automatisierten RIS durch entsprechende DV-technische Vorkehrungen (z.B. auf die Dateiebene bezogene Passworte) umgesetzt werden.

Enthält die HGO wie in diesem Beispiel einschränkende Vorgaben für Datenübermittlungen oder Informationszugriffe, dürfen diese auch nicht auf dem Umweg über gleichsam „allwissende" Fraktionsmitarbeiter umgangen werden. Sicherlich wird den Mandatsträgern in vielen Fällen der Umgang mit dem Ratsinformationssystem erleichtert, wenn für sie die Fraktionsangestellten Datenabfragen vornehmen. Doch dürfen die Mitarbeiter keine generelle bzw. pauschale Zugriffsberechtigung auf alle Dokumente erhalten; Grenze ist immer die Zugriffsbefugnis desjenigen Stadtverordneten, der sie beauftragt hat. Diese Nutzungsbeschränkungen für Hilfskräfte der Gemeindevertreter sind verpflichtend durch Aufnahme in den Arbeitsvertrag, Dienstanweisung o.ä. festzulegen und durch DV- technische Protokollierung überprüfbar zu machen.

Am Beispiel des Kasseler Vorhabens konnten auch weitere Einzelfragen von Ratsinformationssystemen angesprochen und geklärt werden, Fragen, bei denen sich Kommunalrecht und Datenschutzrecht überlappen. Dies gilt beispielsweise für den Umfang der Möglichkeit, personenbezogene Dokumente aus dem RIS abzurufen, die vor der Mandatszeit des Gemeindevertreters entstanden sind. Ebenfalls festgelegt wurde der Zugriff auf Unterlagen nicht-öffentlicher Ausschußsitzungen durch die Stadtverordneten, die diesem Gremium nicht angehören und dementsprechend nur ein Recht der Teilnahme als Zuhörer haben (§ 62 Abs. 4 Satz 3 HGO).

11.3
Stand und weiteres Verfahren

In Kassel befindet sich das RIS-Projekt in der Phase der Umsetzung der übereinstimmend festgelegten Vorgaben. Der Magistrat hat im Dezember 1990 den Beschluß über den Zugriff der städtischen Ämter auf das RIS gefaßt. Über die Nutzungsmodalitäten für die Gemeindevertreter will die Stadtverordnetenversammlung Anfang 1991 entscheiden.

In Wiesbaden erfolgt der Anschluß der Fraktionen an das kommunale Informations- und Dokumentationssystem auf der Grundlage eines Beschlusses des Ältestenausschusses der Stadtverordnetenversammlung, an dessen Formulierung ich beteiligt worden bin. In diesem Beschluß sind der Rahmen der Zugriffsbefugnisse der Fraktionsmitarbeiter ebenso festgelegt wie die besondere Behandlung vertraulicher Sitzungsunterlagen. Da bisher nur Betreffangaben und Beschlüsse gespeichert und für den Abruf bereitgehalten werden, habe ich für weitere Ausbaustufen die Stadt Wiesbaden um erneute Abstimmung gebeten.

12. Umweltschutz

12.1
Datenschutzregelungen im Hessischen Abfallwirtschafts- und Altlastengesetz

Bei der Abfallbeseitigung und im Zusammenhang mit dem Aufspüren, Untersuchen und dem Unschädlichmachen sogenannter Altlasten muß eine große Anzahl von Daten erhoben und weiterverarbeitet werden. Zum nicht geringen Teil sind dies personenbezogene Daten, insoweit es sich nämlich um Daten privater Haushalte, von Handwerks- und Landwirtschaftsbetrieben oder von als Personengesellschaften geführten Unternehmen handelt. Es liegt in der Aufgabe einer effektiven Abfallbeseitigung begründet, daß nur im Zusammenwirken der dafür verantwortlichen Behörden – vor allem der Kommunalverwaltungen und der Fachbehörden des Landes – sowie privater Stellen eine umweltgerechte Abfallbeseitigung und Altlastenbereinigung möglich ist. Wie es sich schon im Bereich der Wasserwirtschaft als notwendig erwiesen hatte (vgl. 18. Tätigkeitsbericht, Ziff. 15.3), ist auch hier eine über die Grundsatzvorschriften des Hessischen Datenschutzgesetzes hinausgehende Datenschutzregelung erforderlich.

Mit dem am 1. Januar 1991 in Kraft getretenen 6. Gesetz zur Änderung des Hessischen Abfallwirtschafts- und Altlastengesetzes vom 19. Dezember 1990 (GVBl. I S. 773) hat der Landtag diese Vorschriften geschaffen. Die Bestimmungen entsprechen dem Gesetzentwurf, den die Landesregierung zuvor mit mir abgestimmt hatte. Während § 24a des neuen HAbfAG allgemein die Datenverarbeitung im Bereich der Abfallentsorgung und Altlastensanierung regelt, enthält die Neufassung des § 17 Abs. 1 HAbfAG nunmehr eine besondere Rechtsgrundlage für die von der Landesregierung geplante „Verdachtsflächendatei". Diese Datei soll in Form eines „Altlastenkatasters" einen Überblick über die Grundstücksflächen mit gefährlichen chemischen Ablagerungen ermöglichen. Gegenüber dem Hessischen Datenschutzgesetz (§ 12 Abs. 2 und 3) erweitert § 24a HAbfAG für die Umweltschutzbehörden die Möglichkeit, Daten ohne Kenntnis des Betroffenen zu erheben. Die Vorschrift über die Verdachtsflächendatei verpflichtet die Gemeinden und Entsorgungspflichtigen, die ihnen vorliegenden Erkenntnisse über Altablagerungen und Altstandorte an das von der Hessischen Landesanstalt für Umwelt zu führende Register zu melden.

12.2
Einsichtsrecht in Umweltakten

Den Entwurf der Fraktion DIE GRÜNEN für ein Gesetz über das Einsichtsrecht in Umweltakten (AERG) vom 19. Juli 1988 (Drucks. 12/2689) haben die beteiligten Landtagsausschüsse Ende 1990 abgelehnt. Eine Entscheidung des Plenums steht noch aus. Zur Vereinbarkeit der Akteneinsicht mit den Erfordernissen des Datenschutzes für die in den amtlichen Unterlagen der Umweltbehörden enthaltenen personenbezogenen Angaben habe ich gegenüber dem Unterausschuß Informationsverarbeitung und Datenschutz eine ausführliche Stellungnahme abgegeben (UID/12/34, Teil II).

Nach meiner Auffassung waren vor allem folgende Punkte des Gesetzentwurfs korrekturbedürftig: Wegen der negativen Erfahrungen in den Vereinigten Staaten ist ein Verbot der kommerziellen bzw. geschäftsmäßigen Nutzung der aus Umweltakten entnommenen persönlichen Daten unverzichtbar. Der Informationszugang muß auf ideelle Zwecke – etwa das Auskunftsinteresse von Anliegern oder Bürgerinitiativen – beschränkt bleiben. Bürger, die bei einer Umweltbehörde eine Anzeige erstattet oder einen Antrag gestellt haben, verdienen Schutz davor, daß sie betreffende personenbezogene Informationen einer unbekannten Vielzahl von möglicherweise in „ihre" Akte Einblick nehmenden Dritten ohne ihre Zustimmung offengelegt werden. Dagegen sollte es nicht zur Voraussetzung des Einsichtsrechts gehören, daß auch die Personalien aller sonstigen in den Akten vorkommenden Personen, etwa Beamte oder Gutachter, geschwärzt werden.

Diese und weitere von mir angeregte Änderungen sind von der Fraktion DIE GRÜNEN akzeptiert und mit dem Änderungsantrag vom 16. Oktober 1990 (Drucks. 12/7505) in die Landtagsberatungen eingebracht worden, so daß datenschutzrechtlich keine Bedenken mehr bestanden.

Trotz der jetzigen Ablehnung der Gesetzesinitiative durch den Landtag ist das Thema Einsichtsrecht in Umweltakten nicht endgültig vom Tisch. Die EG-Richtlinie über den freien Zugang zu Informationen über die Umwelt vom 7. Juni 1990 (Amtsbl. der EG L 158/56) verpflichtet die Mitgliedstaaten der Gemeinschaft, bis zum 31. Dezember 1992 ihren Inhalt in nationales Recht umzusetzen, wobei die Regelungsebene – Bundes- oder Landesrecht – Sache der föderalen Verfassungsordnung in der Bundesrepublik ist. Ich befürworte seit jeher nachhaltig die Ergänzung des Datenschutzes als Abwehrrecht um ein „Recht auf Information" („freedom of information; vgl. dazu 14. Tätigkeitsbericht, Ziff. 11.1). Die EG-Richtlinie schafft die Voraussetzungen für einen ersten, auf den Teilbereich Umwelt konzentrierten Schritt in diese Richtung.

13. Informationsrechte des Bürgers

13.1
Auskunftsverhalten der Sicherheitsbehörden

Das Recht des Betroffenen, Auskunft über die zu seiner Person gespeicherten Daten nach § 18 Abs. 1 des Hessischen Datenschutzgesetzes zu erhalten, wird meist direkt gegenüber der jeweiligen speichernden Stelle geltend gemacht. Nicht selten wenden sich Personen, die annehmen, eine Sicherheitsbehörde habe Daten zu ihrer Person gespeichert, aber auch an den Datenschutzbeauftragten. Sie fordern mich auf festzustellen, ob und welche Erkenntnisse über sie gesammelt wurden und wenn ja, ob dieses Vorgehen rechtmäßig ist; teilweise bitten sie darum, daß ich mich für eine Löschung ihrer Daten einsetze.

Soweit der Betroffene annimmt, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein, ist es ihm unbenommen, sein Auskunftsrecht nach § 18 HDSG gegenüber der speichernden Stelle geltend zu machen oder gem. § 28 HDSG sein Recht, den Hessischen Datenschutzbeauftragten anzurufen, wahrzunehmen. Gleiches gilt bei bereichsspezifisch geregelten Auskunftsrechten, wie z.B. § 29 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung oder § 9 Hessisches Meldegesetz.

Allerdings: Das Auskunftsrecht des Bürgers nach § 18 Abs. 1 unterliegt den Einschränkungen des § 18 Abs. 5 HDSG. Es gilt nicht, wenn die speichernde Stelle nach einer Abwägung feststellt, daß das Auskunftsrecht hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse eines Dritten zurücktreten muß. An diese Entscheidung der Behörde bin auch ich gebunden. Ich kann zwar jedem der Fälle nachgehen und erhalte Auskunft bzw. Einsicht in alle Unterlagen der Behörden. Komme ich aufgrund meiner Nachforschungen zu dem Ergebnis, daß Daten zu einem Betroffenen in unzulässiger Weise verarbeitet wurden, kann ich die Löschung bzw. Vernichtung der Akten verlangen. Dem betroffenen Bürger darf ich allerdings nur in dem Rahmen Auskunft über das Ergebnis meiner Nachforschungen erteilen, in dem dies die Behörde selbst – nach erfolgter Abwägung – tun würde. Dies führt z.B. zu der unerträglichen Situation, daß ich auch dann, wenn keine Erkenntnisse bei der entsprechenden Behörde existieren, dem Betroffenen dies oftmals nicht mitteilen kann.

Das Verhalten der verschiedenen Sicherheitsbehörden ist sehr unterschiedlich. Zeigt sich die Polizei weitgehend auskunftsbereit, geht das Landesamt für Verfassungsschutz in der Mehrzahl der Fälle von einem überwiegenden öffentlichen Geheimhaltungsinteresse aus und läßt eine Auskunftserteilung nicht zu.

13.1.1
Polizei

97 Personen haben mich in der Zeit von 1988 bis Oktober 1990 gebeten festzustellen, ob die Polizei Daten zu ihrer Person gespeichert hat und, falls dies zutrifft, mich beauftragt, die Rechtmäßigkeit der Datenspeicherung zu prüfen.

Großzügig zeigte sich die Polizei in ihrem Auskunftsverhalten gegenüber den Betroffenen. Selbst bei Personen, über die im Bereich „Staatsschutz" Informationen vorlagen, konnte ich – mit Zustimmung der zuständigen Polizeibehörden – die Betroffenen über evtl. vorliegende Datenspeicherungen informieren.

Lediglich in zwei Fällen wurde eine Auskunftserteilung teilweise verweigert. Einmal überwog das öffentliche Geheimhaltungsinteresse, einen Betroffenen über alle zu seiner Person vorliegenden Daten nicht zu informieren. In einem anderen Fall stand das Geheimhaltungsinteresse eines Dritten dem Recht des Auskunftssuchenden darüber informiert zu werden, wer der Polizei einen Hinweis auf seine Person gegeben hatte, entgegen. In beiden Fällen war die Abwägung nach § 18 Abs. 5 HDSG ermessensfehlerfrei erfolgt.

13.1.2
Landesamt für Verfassungsschutz

Ganz anders ist das Auskunftsverhalten des Landesamtes für Verfassungsschutz. Von 1988 bis Oktober 1990 haben sich 61 Personen an mich gewandt, die annahmen, das Landesamt für Verfassungsschutz habe Daten zu ihrer Person gespeichert.

Bei 48 Personen war dies nicht der Fall.

Oft ging aus den Schreiben der Betroffenen hervor, daß sie die Vorstellung, vom Verfassungsschutz beobachtet oder „registriert" zu werden, bzw. ihre Befürchtung, daß ihr Telefonanschluß abgehört werde, in hohem Maße psychisch belastete. In anderen Fällen schilderten die Betroffenen eine besondere Belastung in einem bestimmten Lebensbereich und/oder einen konkreten Anlaß, wonach sie von einer Datenspeicherung durch die Verfassungsschutzbehörde ausgingen.

In beiden Fallgruppen machte ich ein besonderes Auskunftsinteresse der Betroffenen geltend. Nach der von der Verfassungsschutzbehörde nach § 18 Abs. 5 HDSG getroffenen Abwägung konnte ich 15 Anfragern mitteilen, daß sie der Behörde vollkommen unbekannt sind. In neun Fällen konnte ich die Betroffenen darüber informieren, daß ihre Annahme nicht zutraf. So hatte der Verfassungsschutz beispielsweise ihre Teilnahme an einer bestimmten Demonstration nicht registriert und waren die Ablehnungen auf Bewerbungen im öffentlichen Dienst nicht von einer Datenspeicherung durch das Landesamt für Verfassungsschutz verursacht worden.

In 24 Fällen ging die vom LfV vorgenommene Abwägung nach § 18 Abs. 5 HDSG zuungunsten der Betroffenen aus. Obwohl auch diese Personen der Behörde vollkommen unbekannt waren, konnte ich sie lediglich über die Rechtslage und das Ergebnis meiner Feststellungen informieren – nämlich, daß eine Beeinträchtigung ihrer schutzwürdigen Belange die im Widerspruch zu den datenschutzrechtlichen Bestimmungen stünden, nicht vorliegt.

Zu 13 Betroffenen verfügte das Landesamt für Verfassungsschutz über Informationen. 5 der Betroffenen wurden informiert. Dies war meistens darauf zurückzuführen, daß sie ihre Vermutung, das LfV sammle Erkenntnisse zu ihrer Person, mit präzisen Angaben abgestützt hatten. Sie wurden darüber unterrichtet, daß eine Informationssammlung zu ihrer Person existiert. In acht Fällen überwog nach vertretbarer Auffassung des LfV das öffentliche Geheimhaltungsinteresse das Auskunftsinteresse.

13.2
Benachrichtigung nach § 18 Abs. 2 HDSG

13.2.1
Ziel

§ 18 Abs. 2 Hessisches Datenschutzgesetz verpflichtet alle öffentlichen Stellen, die personenbezogenen Daten in einer automatisierten Datei speichern, die Betroffenen davon schriftlich zu benachrichtigen. In der Benachrichtigung müssen folgende Angaben enthalten sein:

1. die Zweckbestimmung der Datei,
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
3. der Kreis der Betroffenen,
4. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und die Herkunft regelmäßig empfangener Daten,
5. die Fristen für die Sperrung und Löschung der Daten.

Der Gesetzgeber hat mit der Pflicht zur Benachrichtigung den Bürger dabei unterstützen wollen, die ihn betreffende Datenverarbeitung der Verwaltung verläßlich zu überblicken. Erst dann kann er seine Auskunfts- oder Einsichtsrechte wirklich ausüben.

13.2.2
Fehlentwicklung

Dieses Ziel der Benachrichtigungspflicht ist nur bedingt erreicht worden. Das liegt nicht zuletzt daran, daß wichtige Bereiche des Verwaltungshandelns von der Benachrichtigungspflicht ausgenommen sind – z.B. Verfassungsschutz oder Sozialverwaltung. Gerade dort, wo die Rechte der Bürger besonders intensiv tangiert sein können, erhalten sie entsprechende Informationen nicht. In anderen wichtigen Bereichen, etwa bei Bußgeldbescheiden oder Besoldungsmitteilungen, ergibt sich meist schon aus der Gestaltung der Bescheide, daß diese aufgrund automatisierter Datenverarbeitung erstellt worden sind. Hier wäre es auch ohne zusätzliche Benachrichtigung möglich, gezielt Auskunfts- und Einsichtsrechte geltend zu machen.

Der angestrebte Zweck der Benachrichtigung wird nur in einigen Bereichen erfüllt und dies sind zum größeren Teil solche, die die Betroffenen weniger als eine Beeinträchtigung ihrer Interessen empfinden.

Die Praxis läßt daher leicht den Eindruck entstehen, als handele es sich bei der Benachrichtigung nur um ein lästiges Übel. Dies wird im Bewußtsein der Bürger häufig noch verstärkt durch die bürokratische Gestaltung der Benachrichtigungstexte.

13.2.3
Notwendigkeit einer Gesetzesänderung

Damit die Benachrichtigung ihrem ursprünglichen Zweck gerecht werden kann, ist eine Korrektur der gesetzlichen Regelung erforderlich. Die Bürger sollten zwar auch künftig benachrichtigt werden. Die weitere Entwicklung der

Datenverarbeitung muß jedoch ebenso wie die zunehmende Vertrautheit der Bürger mit den neuen Technologien Anlaß sein, Zweck und Umsetzung getroffener gesetzlicher Regelungen zu überprüfen und wo notwendig weiter zu entwickeln. Insbesondere kommen folgende Änderungen und Klarstellungen in Betracht:

13.2.3.1
Durchführung der Benachrichtung

Ein nicht unwesentlicher Teil der auftretenden Probleme bei der Durchführung der Benachrichtigung ist schon auf der Grundlage der jetzigen Regelung leicht zu vermeiden.

Oft werden die durch die große Anzahl der Benachrichtigungsfälle anfallenden Kosten beklagt. Es ist unbestritten, daß die Verwaltung mit den vorhandenen Mitteln sparsam umgehen muß.

Sparsamkeit kann aber nicht ein Grund für die Einschränkung der Rechte der Bürgerinnen und Bürger sein. Bei einer sinnvollen Gestaltung des Verfahrensablaufes sind jedoch auch Kosteneinsparungen möglich.

13.2.3.1.1
Verständlichkeit von Bescheiden

Eine Benachrichtigung kann ihren Zweck nur erfüllen, wenn sie für Laien verständlich ist. Hier gilt es wie bei jeder anderen Mitteilung, auf Bürgerfreundlichkeit zu achten. Es ist nicht damit getan, den eingangs beschriebenen Datensatz aufzulisten. Zur Verständlichkeit trägt auch bei, dem Bürger zu erläutern, weshalb er eine solche Mitteilung erhält. Die gängige Floskel „gemäß § 18 Abs. 2 HDSG benachrichtige ich Sie, daß folgende Daten..." schafft wenig zusätzliche Klarheit. Dabei ist ggf. in Kauf zu nehmen, daß eine ernsthaft ausformulierte Benachrichtigung eben nicht in wenigen Zeilen am untersten Rand eines Verwaltungsbescheides unterzubringen ist.

Die nachfolgend abgedruckte vorbildliche Benachrichtigung hat der Hessische Rundfunk 1990 an seine Hörer versandt:

Original Benachrichtigung GEZ

GEZ

Benachrichtigung gemäß § 18 Abs. 2 des Hessischen Datenschutzgesetzes

Herrn
Prof. Dr. Spiros Simitis

Sehr geehrte Rundfunkteilnehmerin, *
sehr geehrter Rundfunkteilnehmer,

gemäß § 18 Abs. 2 des Hessischen Datenschutzgesetzes HDSG haben wir die Rundfunkteilnehmer darüber zu benachrichtigen, daß im Rahmen des Rundfunkgebühreneinzugs personenbezogene Daten in einer automatisierten Datei gespeichert werden. Nach § 42 Abs. 1 HDSG müssen auch die Personen benachrichtigt werden, deren Daten bereits beim Inkrafttreten des HDSG am 1. Januar 1987 gespeichert waren. Mit den auf der Rückseite dieses Schreibens enthaltenen Informationen kommen wir dieser Verpflichtung nach.

Die GEZ nimmt als gemeinsames Rechenzentrum der Landesrundfunkanstalten und des Zweiten Deutschen Fernsehens den Einzug der Rundfunkgebühren wahr. Rechtsgrundlage hierfür ist der Staatsvertrag über die Regelung des Rundfunkgebührenwesens vom 5. 12. 1974 (Gesetz- und Verordnungsblatt für das Land Hessen 1975, Seite 135). Ausschließlich zum Zwecke des Rundfunkgebühreneinzugs werden Daten aller Rundfunkteilnehmer bei der GEZ gespeichert und verarbeitet. Dabei handelt es sich abhängig von den Gegebenheiten des jeweiligen Einzelfalles um

- Anschriftendaten
- Daten über die Anzahl der gemeldeten Hörfunk- und Fernsehgeräte
- Daten über die Zahlungsweise und die Kontoverbindung
- Daten über die Zahlungen und Erstattungen
- Daten über Anmeldung, Abmeldung, Befreiung von der Rundfunkgebührenpflicht und Schriftwechsel mit dem Rundfunkteilnehmer
- Daten zu Mahnmaßnahmen
- Daten zu Ordnungswidrigkeitsverfahren.

Bei Teilnahme am Lastschriftverfahren ist regelmäßig bei Fälligkeit der Rundfunkgebühren eine Datenübermittlung an das zuständige Geldinstitut erforderlich. Umgekehrt werden auch Informationen über Zahlungen von Rundfunkteilnehmern von den Geldinstituten an die GEZ weitergeleitet.

Die Daten abgemeldeter Rundfunkteilnehmer werden innerhalb eines Jahres ab dem Ende des Jahres, in dem die Abmeldung durchgeführt wurde, gelöscht.

Mit freundlichen Grüßen
Ihr Hessischer Rundfunk

13.2.3.1.2
Zeitpunkt der Benachrichtigung

Einen ausdrücklichen Zeitpunkt, zu dem die Benachrichtigung erfolgen muß, schreibt das Gesetz nicht vor. Es stellt lediglich klar, daß die Benachrichtigung schon im Zeitpunkt der Erhebung erfolgen kann. Dies ist aber vor allem in Fällen, in denen Bürger nicht zu einer Auskunftserteilung aufgefordert werden, nicht möglich. Wendet sich ein Bürger an eine Behörde mit einer Bitte oder Eingabe, erfolgt meist die automatisierte Verarbeitung seiner Daten bevor er von der Behörde in irgendeiner Form eine Mitteilung bekommt. Selbstverständlich erfüllt die Benachrichtigung nur ihren Zweck, wenn sie zeitnah mit der automatisierten Verarbeitung erfolgt. Nur dann ist es z.B. möglich, frühzeitig das Auskunftsrecht und ggf. Berichtigungsansprüche geltend zu machen. Andererseits werden in der Mehrzahl der hier betroffenen Fälle, die Daten automatisiert verarbeitet, die der Bürger von sich aus der Verwaltung mitgeteilt hat. Deshalb kann die Benachrichtigung auch zusammen mit der Antwort an den Betroffenen erfolgen. Wichtig ist, die Verwaltungsabläufe so zu gestalten, daß in jedem Fall eine Benachrichtigung erfolgt. Allerdings ist ein angemessener zeitlicher Zusammenhang zwischen der Kontaktaufnahme des Bürgers mit der Verwaltung und der Antwort der Verwaltung erforderlich.

Bei einer Vielzahl von Dateien, gerade solchen, die der Organisation des Verwaltungsablaufes dienen, ist es nicht ausgeschlossen, daß vor Ablauf der Löschungsfrist erneut ein Anlaß entsteht, der die Benachrichtigungspflicht auslöst. So halte ich es z.B. nicht für zwingend erforderlich, daß bei einer Geschäftsstellendatei eines Gerichtes jeder Klageeingang erneut zu einer Benachrichtigung der am Verfahren beteiligten Anwälte führt, wenn sichergestellt ist, daß bei der ersten Speicherung eine Benachrichtigung erfolgt, in der auch diese Möglichkeit deutlich dargelegt wird. Bei jeder Datei ist insoweit abzuwägen, unter Berücksichtigung des betroffenen Personenkreises und der Art der verarbeiteten Daten, ob eine solche Vereinfachung gerechtfertigt sein kann.

13.2.3.1.3
Fehlende Anschrift für eine Benachrichtigung

Die Benachrichtigung kann ihren Zweck nur erreichen, wenn sie dem einzelnen Bürger zugeht. Dies bedeutet, daß im Einzelfall für eine Benachrichtigung mehr Daten benötigt würden, als in der Datei, die die Benachrichtigungspflicht auslöst, selbst gespeichert werden sollen. Das ist z.B. der Fall bei einem automatisierten Terminkalender eines Bürgermeisters, bei dem lediglich Name und Zweck eines verabredeten Termins aber nicht die Anschrift oder weitere Angaben über den Gesprächspartner im Terminkalender gespeichert werden.

Die Benachrichtigungspflicht kann nicht Rechtsgrundlage für die Erhebung zusätzlicher Daten sein. Auch eine Zweckänderung bezogen auf andere Dateien, die ggf. die fehlenden Angaben enthalten, ist unzulässig. Fehlende Angaben dürfen deshalb weder zusätzlich erhoben noch einer Datei, die für andere Zwecke besteht, entnommen werden. In den Fällen, in denen sich vor der Benachrichtigung die Anschrift des Betroffenen geändert hat, darf die nunmehr aktuelle Anschrift auch nicht nachrecherchiert werden.

13.2.3.1.4
Dateien, deren Zweck durch eine Benachrichtigung verloren gehen könnte

Die Benachrichtigung darf nicht dazu führen, daß die Verwaltung ihrem gesetzlichen Auftrag nicht mehr nachkommen kann. So legt § 18 Abs. 5 HDSG ausdrücklich fest, daß die Benachrichtigung entfällt, wenn eine Abwägung ergibt, daß die Rechte der Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung zurücktreten müssen. Das kann nicht nur in den klassischen Fällen wie etwa bei der Strafverfolgung der Fall sein. Denkbar ist dies z.B. auch in Bereichen, wo zur Vollstreckung von Forderungen Angaben vorgemerkt werden, um ggf. in einiger Zeit Forderungen niederzuschlagen, weil Pfändungsmöglichkeiten nicht gegeben sind. In diesem Beispiel würde durch eine Benachrichtigung die Zahlungsbereitschaft vieler Schuldner sinken. Da der Gesetzgeber davon ausging, daß die Ausnahmeregelung des § 18 Abs. 5 HDSG restriktiv auszulegen ist, muß die datenverarbeitende Stelle in jedem Einzelfall sorgfältig eine solche Abwägung treffen und begründen.

13.2.3.1.5
Kreis der zu benachrichtigenden Personen

Bei einer Vielzahl von Verwaltungsvorgängen macht der Bürger auch Angaben über andere Personen, weil sonst keine Entscheidung möglich ist. So ist z.B. für die Berechnung der Besoldung bei Beamten auch die Angabe von Daten über Ehepartner und Kinder notwendig. Auch diese Daten werden automatisiert verarbeitet. In vielen Fällen wären zur Benachrichtigung aller auch nur mittelbar betroffener Personen, zusätzliche Informationen erforderlich. Hier ist die Pflicht zur Benachrichtigung restriktiv vorgangsbezogen anzuwenden. Zu benachrichtigen ist jeweils der Hauptbetroffene. Dies ist im Regelfall die Person, die die Angaben macht oder für die ein Antrag aufgenommen wird. Das Auskunftsrecht aller Betroffenen wird dadurch jedoch nicht eingeschränkt.

13.2.3.2
Absehen von der Benachrichtigung

Aufgrund der derzeitigen Regelung sind jedoch auch noch Konstellationen vorhanden, in denen der Aufwand für die Benachrichtigung und der damit erreichte Zweck – auch unter Berücksichtigung des durch die Verarbeitung der

personenbezogenen Daten im konkreten Zusammenhang entstehenden Gefährdungspotentials – in einem offensichtlichen Mißverhältnis stehen. Hier halte ich es für gerechtfertigt, für einzelne Dateien sorgfältig abzuwägen, ob die Benachrichtigung nicht entbehrlich ist, ohne daß die Gefahr einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung entsteht.

Dies gilt allerdings nur für die Benachrichtigung. Selbstverständlich bleiben alle Rechte der Betroffenen (z.B. Auskunfts- oder Berichtigungsansprüche) ebenso bestehen, wie die übrigen Verpflichtungen der datenverarbeitenden Stellen (Beachtung der Zweckbindung, Einhaltung der erforderlichen Datensicherungsmaßnahmen usw.).

13.2.3.2.1
Textverarbeitung

Schriftstücke werden heute zunehmend mit Textverarbeitungsprogrammen auf PCs erstellt. Die Folge: Jeder einzelne Brief ist eine Datei im Sinne von § 2 Abs. 5 Ziff. 1 HDSG.

Die mit der automatisierten Datenverarbeitung verknüpfte Gefährdung des Kontextverlustes bzw. einer nicht mehr überschaubaren Zweckänderung entsteht in der Regel jedoch erst dann, wenn die Datentechnik gleichzeitig auch für andere Funktionen als die lediglich technische Herstellung von Schreiben verwendet wird. Solche Dateien können z.B. mit Hilfe der Textverarbeitungsprogramme sortiert, in ihnen kann nach einzelnen Angaben, wie Namen, gesucht werden usw. Diese Funktionen können u.a. für Zwecke der Büroorganisation genutzt werden. So läßt sich etwa der Postein- und -ausgang überwachen oder die Registratur der Vorgänge unterstützen. Diese Erweiterung vom technischen Erstellen von Dokumenten zur Nutzung der Datenverarbeitung für die Bürokommunikation stellt Verarbeitungszusammenhänge her, die ein Bürger nicht ohne weiteres erwartet. Findet eine solche Verknüpfung statt, ist eine Benachrichtigung auch weiterhin erforderlich. Bei reiner Textverarbeitung dagegen ist eine Benachrichtigung nicht sinnvoll.

13.2.3.2.2
Adresslisten für Materialversand

Eng mit der Textverarbeitung verbunden ist eine Fülle von Dateien, die der Öffentlichkeitsarbeit der Behörden dienen. Dazu gehören etwa Listen der Presseorgane bzw. Journalisten ebenso wie die Anschriften von Bürgern, die regelmäßig Informationsmaterial erhalten sollen oder an kulturellen Veranstaltungen interessiert sind. In aller Regel bitten die Betroffenen selbst um Aufnahme in diese Listen. Soweit sich solche Verteiler auf Anschriften beschränken und eine Verknüpfung mit anderen Datenbeständen nicht stattfindet, ist ein Verzicht auf eine Benachrichtigung möglich.

13.2.3.2.3
Kurzfristig bestehende Dateien

Vor allem Arbeitsplatzcomputer werden häufig eingesetzt, um einmalig anfallende Arbeiten zu erleichtern, für die ein dauerhafter Datenbestand nicht notwendig ist. Beispiele dafür sind etwa die Organisation von Sportfesten an Schulen oder die Anmeldung für Veranstaltungen. Nach Abschluß der Veranstaltung besteht kein Interesse mehr, die entsprechenden Daten weiterhin zu speichern. Nach der deshalb sofort erfolgten Löschung der Daten kann auch das Auskunftsverlangen des Betroffenen nicht mehr erfüllt werden. Die Benachrichtigung ginge ins Leere. Dies trifft vor allem für solche Fälle zu, wo die einzelne Aufgabe in weniger als 2 Monaten erledigt ist.

13.2.3.2.4
Daten der Bearbeiter von einzelnen Vorgängen

Im Rahmen der zunehmenden Automatisierung der Verwaltung steigt auch die Anzahl der Verfahren, bei denen zusätzlich zu den notwendigen Angaben der Bürger, Angaben über den diese Angelegenheit betreuenden Bediensteten mitverarbeitet werden, z.B. um im Anschreiben an den Bürger den zuständigen Sachbearbeiter zu benennen, oder um für den internen Verwaltungsablauf den jeweils handelnden Mitarbeiter kenntlich zu machen.

Im Unterschied zum Bürger ist dem Mitarbeiter sowohl die Tatsache der automatisierten Verarbeitung, als auch in aller Regel der Umfang der verarbeiteten Daten bekannt. Der Sachbearbeiter ist nicht Hauptbetroffener.

Transparenz der Vorgänge und Information der Betroffenen sind hier zusätzlich auf andere Weise sichergestellt: Der Sachbearbeiter veranlaßt in aller Regel selbst die entsprechende Speicherung bzw. führt die Verarbeitung selbst durch; bei der Einführung des Verfahrens ist der Personalrat beteiligt. Durch diesen erfolgt auch eine zusätzliche Kontrolle im Rahmen der Wahrnehmung seiner Verpflichtung, die Einhaltung aller Datenschutzregelungen, die dem Schutz der Beschäftigten dienen, zu überwachen. Die Bearbeiter müssen daher nicht benachrichtigt werden.

14. ISDN (Integrated Services Digital Network)

14.1
Berichtsantrag der SPD-Fraktion

Der Berichtsantrag der SPD-Fraktion zur Anwendung des neuen ISDN- Netzes der Bundespost in Hessen (Drucks. 12/4812) ist 1990 in mehreren Ausschüssen (weiter-)behandelt worden. Dazu hatte ich bereits 1989 ausführlich Stellung genommen (vgl. 18. Tätigkeitsbericht, Ziff. 16.2.1 bis 16.2.4). Die Landesregierung hat in ihren beiden Ausschußvorlagen vom 20.11.1989 (Hauptausschuß 12/42) und vom 07.08.1990 (Hauptausschuß 12/58) ihre Auffassung bekräftigt, das Land habe keine Kompetenz zur Herstellung sozialverträglicher Einsatzbedingungen für das ISDN, für ein entsprechendes eigenes hessisches Konzept bestehe daher kein Anlaß. Die Notwendigkeit besonderer Vorkehrungen für die Nutzung des ISDN durch die Landesbehörden könne die Landesregierung generell nicht erkennen.

Zu dieser Position habe ich auf die Bitte des Innenausschusses hin mit Schreiben vom 22. August 1990 eine ergänzende Stellungnahme abgegeben. Das Land Hessen hat sehr wohl ein breites Instrumentarium zur Verfügung und sollte es auch nutzen, um den – in meiner ersten Stellungnahme im einzelnen dargestellten – spezifischen Risiken des ISDN mit einem Gesamtkonzept zur Sicherung der „Sozialverträglichkeit" für Bürger und Bedienstete zu begegnen. Zu diesen Instrumenten gehören Gesetzgebungsbefugnisse für die Regelung der Nutzung der über das ISDN laufenden Telekommunikationsdienste, und zwar generell oder zumindest für die Nutzung durch die öffentlichen Stellen des Landes und der Kommunen. Beispiele für den Gebrauch dieser Landeskompetenz sind der Bildschirmtext-Staatsvertrag von 1983 oder die Bestimmung des § 36 HDSG über das Erfordernis der Einwilligung des Betroffenen beim Einsatz von Fernmeß- oder Fernwirksystemen durch hessische Dienststellen.

Bestandteil eines solchen Konzepts wären auch die Mitwirkungsmöglichkeiten des Landes bei der auf das ISDN bezogenen Bundesgesetzgebung, insbesondere bei den nach dem Poststrukturgesetz zu erlassenden Datenschutzverordnungen, die der Zustimmung des Bundesrats bzw. des Infrastrukturrats bedürfen (s. dazu Ziff. 16.5.1). Der Hessische Wirtschaftsminister hat zwischenzeitlich sowohl im Infrastrukturrat als auch in der Wirtschaftsministerkonferenz auf die Notwendigkeit hingewiesen, das Thema „Datenschutz im ISDN" in diesen Gremien zu beraten (vgl. Hauptausschußvorlage 12/66 vom 12.11.1990).

Handlungsspielraum aber hat die Landesregierung vor allem im Bereich ihrer eigenen Organisationshoheit; hier kann sie per Kabinettsbeschluß, Erlaß o.ä. Vorgaben machen, um bei der Anschaffung und Verwendung von an das ISDN angeschlossenen Geräten der Informationstechnik den Datenschutz, aber auch die Arbeitsplatzsituation und die Bürgerfreundlichkeit zu verbessern. Diese auf die konkreten Einsatzbedingungen gerichteten Maßnahmen müssen die notwendigerweise allgemeiner gehaltenen ISDN-bezogenen Regelungen durch Gesetz oder Verordnung ergänzen. Die Aussage der Landesregierung, besondere Vorkehrungen des Landes zur Nutzung des ISDN-Netzes seien überflüssig, wenn der Bund derartige Regelungen treffe, vermengt die beiden Aktionsebenen der Gesetzgebung einerseits und der praktischen Einsatzbedingungen andererseits und geht daher fehl.

14.2
ISDN-fähige Anlagen

Sofort tätig werden muß die Landesregierung vor allem im Hinblick auf die ISDN-fähigen Nebenstellenanlagen, die sich bei Landesbehörden und Kommunen immer mehr ausbreiten (dazu 18. Tätigkeitsbericht, Ziff. 16.2.5). Viele Verwaltungen wollen aus verschiedenen, auch aus Datenschutzgründen, nicht alle vom Hersteller angebotenen Leistungsmerkmale der ISDN-Telefonanlage nutzen.

Wenn es dann darum geht, die technischen und organisatorischen Maßnahmen zu treffen, um den Betrieb nur im gewünschten Umfang zuzulassen, treten häufig Schwierigkeiten auf. Dies hat auch eine Ursache in der Verkaufspolitik der Hersteller: Angeboten werden umfangreiche, komfortable Anlagen als Komplettangebot für Hard- und Software. Zusatzaufwand und damit Mehrkosten entstehen dann nicht etwa durch Extrawünsche, sondern im Gegenteil durch den Verzicht auf einen Teil des Leistungsangebotes, eine Herstellerphilosophie, die im übrigen auch für viele andere „Standardanwendungen" gilt. Dies erschwert es, den Verarbeitungsumfang auf das für den Verwendungszweck notwendige und von Dienststellenleitung und Personalrat gewünschte Maß zu beschränken.

Bei den Stellungnahmeverfahren im Rahmen des § 34 Abs. 5 HDSG gibt es daher häufig Meinungsverschiedenheiten über die Fragen, wie umfangreich die technischen und organisatorischen Maßnahmen nach § 10 HDSG sein müssen, und was erforderlich ist, um einen ordnungsgemäßen Betrieb der Anlage sicherzustellen und nachvollziehbar zu machen. Auch hier sind die Hersteller gefragt, die entsprechende technische Unterstützung für die Realisierung von Revisionsanforderungen zu leisten.

Für die ISDN-Anlage der Hochschulregion Darmstadt wurde 1990 ein Revisionskonzept entwickelt. Darin wird der Umfang von Protokollierung und Dokumentation beschrieben und eine Hilfestellung für die Auswertung solcher Unterlagen gegeben. Vergleichbare Konzepte halte ich für jedes ISDN-fähige System, ja für jede größere DV-Anwendung für unverzichtbar.

Aus dem Finanzministerium verlautete im Dezember 1990, daß derzeit dort die Fernsprechvorschriften für die hessische Landesverwaltung überarbeitet werden und die Änderungsvorschläge den Ressorts und mir im Januar 1991 zur Stellungnahme zugehen sollen. Vorgesehen seien dabei auch spezielle Datenschutzbestimmungen für Nebenstellenanlagen in den Landesbehörden.

15. Datensicherheit

15.1
Datensicherheit durch technische und organisatorische Maßnahmen

„Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind,
1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. . . ."

Wer in der öffentlichen Verwaltung personenbezogene Daten automatisiert oder auch manuell verarbeitet, sollte sie eigentlich kennen, die „Zehn Gebote" des Datenschutzes. Gemeint sind die technischen und organisatorischen Maßnahmen des § 10 HDSG. Sie sind, seit 1978 im Wortlaut fast unverändert, ein wesentlicher Bestandteil der gesetzlichen Regelungen zur Gewährleistung des Datenschutzes und der Datensicherheit. Ob es sich um Fragen der Objektsicherung von Gebäuden oder Räumlichkeiten mit Datenverarbeitungsanlagen handelt, die unberechtigte Kenntnisnahme von Daten bzw. Informationen verhindert werden soll oder die Integrität von Programmen zur Verarbeitung von Daten zur Debatte steht, immer führt die Klärung der aufgeworfenen Fragen zu den Vorschriften des § 10.

Gemessen am Umfang der inzwischen veröffentlichten Literatur zu diesem Themenkreis sollte man annehmen, das Problem der Datensicherheit sei im Bewußtsein der mit Datenverarbeitung beschäftigten Mitarbeiter fest verankert. In den Tätigkeitsberichten finden sich jedoch immer wieder Hinweise darauf, daß dies nicht der Fall ist (vgl. beispielsweise 15. TB, Ziff. 9.4 u. 9.5, 17. TB, Ziff. 12. und 18. TB, Ziff. 17.). Umfragen bei den Betreibern von Rechenzentren und Anwendern von DV-Verfahren zeigen, daß die Mehrzahl der befragten Personen ein hohes Gefährdungspotential ihrer Daten, Programme und Maschinen für sehr wahrscheinlich hält. Gleichzeitig räumen sie aber ein, daß die Bereitschaft zu Investitionen im Bereich der Datensicherheit nach wie vor gering ist.

Die wesentlichen Erkenntnisse aus meiner Prüfpraxis, die regelmäßig Bestandteil der Tätigkeitsberichte sind, hat jetzt auch der Bundesrechnungshof in seinem diesjährigen Bericht über Prüfungen bei den Bundesbehörden bestätigt:

- Es fehlen vernünftige Sicherungskonzepte z.B. gegen Katastrophen oder Sabotage.
- Risikoanalysen werden nicht erstellt bzw. bleiben ohne Konsequenzen.
- Zugangs-, Benutzer- und Zugriffskontrollen sind lückenhaft.
- Zugriffsberechtigungen werden nicht restriktiv sondern zu großzügig erteilt.
- Systemtechniker haben ungehinderten Zugriff zu allen Produktionsdaten und werden bei Wartungsarbeiten nicht beaufsichtigt.
- Vorhandene Teillösungen existieren nur auf dem Papier und haben oft reine Alibifunktion.
- Überprüfungen der Sicherungsmaßnahmen finden nicht statt.
- Die Mitarbeiter zeigen für die Probleme des Datenschutzes nur wenig oder überhaupt keine Sensitivität.

Auch diesmal soll am Beispiel ausgewählter Vorfälle aus dem Berichtszeitraum aufgezeigt werden, wo die Defizite sind.

Vorab: Kein Fall ist völlig neu. So oder in ähnlicher Form gab es sie auch schon früher. Die Ursachen und ihre Folgen sind stets die gleichen. Die Einsicht der Verantwortlichen kommt wie immer zu spät. Trotz dieses eher pessimistischen Ergebnisses gibt es die Möglichkeit die Situation langfristig zu verbessern: Der Datenschutz muß im Bewußtsein der verantwortlichen Mitarbeiter einen höheren Stellenwert erlangen. Dies ist letztlich nur durch kontinuierliche Information und Kontrollen zu erreichen.

15.2
Unverschlossene Staatskasse Wiesbaden

Aus dem Wiesbadener Tagblatt erfuhr ich, daß am Abend des 16.07.1990 um 21.15 Uhr Passanten festgestellt hatten, daß ein Eingang des Gebäudes, in dem die Staatskasse Wiesbaden untergebracht ist, unverschlossen war und die Räume der Staatskasse für jeden frei zugänglich waren. Ich habe daraufhin den Leiter der Staatskasse um Stellungnahme gebeten. Dieser bestätigte, daß das Gebäude an dem fraglichen Abend tatsächlich frei zugänglich war. Zwar sei der Haupteingang des Gebäudes, der gleichzeitig der Eingang zur Staatskasse sei, verschlossen gewesen, jedoch habe der zweite Hauseingang, der von den im Hause ansässigen Privatfirmen genutzt werde, offen gestanden. Die Etagentüren, die die Flure der Staatskasse vom Treppenhaus trennen, seien ebenfalls unverschlossen gewesen. Auch die Zimmertüren seien – bis auf wenige Ausnahmen – nicht abgeschlossen gewesen. Der Vertreter des Hausmeisters habe offensichtlich nicht gewußt, daß es zu seinen Aufgaben gehört, die Etagentüren der Staatskasse zu verschließen.

Bei einer anschließenden von meinen Mitarbeitern an Ort und Stelle vorgenommenen Überprüfung zeigten sich eine Reihe von Mängeln.

15.2.1
Mängel:

Ein wesentliches Problem bestand darin, daß sowohl die Eingangstür wie auch die Etagentüren zu den Fluren der Staatskasse vom Hausmeister zu einer Zeit aufgeschlossen wurden, zu der noch kein Mitarbeiter der Staatskasse im Hause anwesend war. Das gleiche galt für das Verschließen der Türen am Abend.

Die einzelnen Zimmertüren blieben nachts größtenteils unverschlossen, weil für jedes Zimmer nur ein Schlüssel existierte, aber die meisten Zimmer von mehreren Mitarbeitern genutzt wurden. Die Räume konnten daher leicht von Unbefugten betreten werden.

Das Problem wurde im konkreten Fall noch dadurch verschärft, daß mehrere Etagen des Gebäudes von Privatfirmen angemietet sind. Die Mitarbeiter dieser Firmen besitzen alle einen Schlüssel für den Nebeneingang. Sie können durch diesen Zugang sowohl das Treppenhaus, als auch die Fahrstühle erreichen, so daß für sie das Betreten der Etagen der Staatskasse ohne weiteres möglich ist.

Neben diesen eher organisatorisch zu lösenden Problemen waren auch erhebliche Mängel bei der Ausstattung festzustellen. Dies betraf einmal die Türen, deren Türschließer zum Teil so mangelhaft funktionierten, daß die Türen nicht ins Schloß fielen und damit ein ungehinderter Zugang von außen möglich war. Zudem waren die Büroräume zum größten Teil mit alten Holzschränken mit Rolltüren ausgestattet, die, selbst wenn sie abschlossen werden, jederzeit leicht auch ohne Schlüssel zu öffnen sind.

Im Eingangsbereich der Staatskasse befinden sich neben der Telefonzentrale auch die Postfächer der einzelnen Bediensteten. Es handelt sich hier um offene Regalfächer, die nicht verschließbar sind. Zum Zeitpunkt des Besuchs lagen in diesen Fächern u.a. „offene" Beihilfeunterlagen.

15.2.2
Forderungen:

Von der Staatskasse habe ich deshalb folgende Maßnahmen zur Verbesserung der Datensicherheit gefordert:

- Es muß sichergestellt sein, daß die Flure in den einzelnen Etagen, über die man die Diensträume erreicht, nur noch zu den Dienstzeiten geöffnet werden, so daß ein Zugang für Unberechtigte nicht möglich ist.

- Für jeden Mitarbeiter ist ein Schlüssel für sein Dienstzimmer zur Verfügung zu stellen. Wenn sich kein Mitarbeiter mehr im Dienstzimmer aufhält, ist das Zimmer zu verschließen.

- Die Türen selbst sind mit einbruchsicherem Glas auszustatten. Die Türschließer müssen ausreichend stark eingestellt sein.

- Es ist weiterhin sicherzustellen, daß im Eingangsbereich bei den Postregalen und an der Telefonzentrale ständig ein Mitarbeiter der Staatskasse anwesend ist. Unterlagen mit sensiblen Daten – wie z.B. Beihilfeunterlagen – dürfen nicht offen in die Postregale gelegt werden. Dies ist per Dienstanweisung zu regeln.

Soweit Sicherheitsprobleme darin mitbegründet sind, daß auch Privatfirmen das Haus benutzen und der Vermieter des Hauses eine private Gesellschaft ist, habe ich betont, daß für die Datensicherheit in der Staatskasse diese allein die Verantwortung trägt und die nötigen Datensicherheitsmaßnahmen zu treffen hat. Dem Finanzminister habe ich mitgeteilt, daß wegen der Schwere der festgestellten Mängel sofort Mittel für die Beseitigung bereitgestellt werden müssen.

15.3
Entsorgungskonzepte

Im Sommer 1990 übergab mir ein Journalist zahlreiche Schriftstücke mit zum Teil hochsensitiven personenbezogenen Angaben wie ärztliche Atteste, Einkommensnachweise, Mietverträge und Wohngeldbescheide. Die Unterlagen stammten zum größten Teil aus öffentlich zugänglichen und unverschlossenen Papier- und Müllcontainern. Der Journalist hatte sie dort entdeckt, als er für eine Fernsehsendung recherchierte, die zeigen sollte, wie Behörden und private Stellen mit personenbezogenen Daten von Bürgern bzw. ihrer Klienten umgehen, genauer gesagt, was mit den Unterlagen nach Gebrauch geschieht.

Da ein großer Teil des Materials aus dem Amt für Wohnungswesen der Stadt Frankfurt stammte, habe ich umgehend die Praxis der Aktenvernichtung in diesem Amt überprüft und dabei folgende Mängel festgestellt:

In dem Amt fallen täglich größere Mengen Unterlagen an, die für die weitere Sachbearbeitung nicht benötigt werden. Dies sind zum Beispiel Durchschriften von Belegen, Entwürfe von amtlichen Schreiben bzw. Verfügungen oder nicht benötigte Anlagen. Diese gelangten dann über die Papierkörbe zum normalen Hausmüll in Müllcontainer. Die unverschlossenen Container standen frei zugänglich neben dem Dienstgebäude und eine besondere Ironie: an den Containern waren Schlösser, diese wurden aber nicht benutzt.

Das Amt für Wohnungswesen hatte ich bereits 1984 überprüft, nachdem erstmals amtliche Unterlagen in der Öffentlichkeit aufgetaucht waren. Damals waren die Mitarbeiter dienstlich belehrt worden, daß Vorgänge mit personenbezogenen Daten nur noch zerkleinert in die Papierkörbe geworfen werden dürfen. Diese Amtsverfügung wurde aber, so stellte sich heraus, nicht genügend beachtet bzw. wurden die Vorgänge nur einmal durchgerissen und waren damit leicht zu rekonstruieren.

Im Dienstzimmer des Hausmeisters steht ein Aktenvernichter. Ist der Hausmeister – was öfters vorkommt – dienstlich unterwegs, kann diese Maschine nicht benutzt werden. Bei meiner Prüfung war im übrigen der Aktenvernichter weder an den elektrischen Strom angeschlossen noch mit einem Sack für die Papierabfälle ausgerüstet, so daß anzunehmen war, daß er über längere Zeit nicht benutzt worden war.

Ich habe den Oberbürgermeister der Stadt Frankfurt auf den Verstoß gegen § 10 Abs. 2 HDSG hingewiesen. Die Vorschrift verlangt ausreichende Maßnahmen um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung der Akten zu verhindern. Außerdem habe ich den Oberbürgermeister aufgefordert sicherzustellen, daß die städtischen Ämter künftig die vom Hessischen Datenschutzgesetz verlangten Datensicherungsmaßnahmen treffen. Zu beachten ist insbesondere:

Datenträger wie Magnetplatten (auch Disketten), Magnetbänder, Carbonbänder, Computerlisten, Einzelausdrucke aber auch sonstige Schriftstücke mit personenbezogenen Daten sind vor unberechtigtem Zugriff bzw. unbefugter Kenntnisnahme zu schützen. Während der Verarbeitung in DV-Systemen oder beim Sachbearbeiter geschieht dies in der Regel durch aufwendige technische und organisatorische Maßnahmen. Nichts anderes gilt für die ordnungsgemäße Entsorgung (Vernichtung) dieses Materials:

- Auf dem gesamten Weg vom Sachbearbeiter bis zum Aktenvernichter oder dem verschlossenen Container müssen die angeordneten Sicherungsmaßnahmen lückenlos greifen. Dies gilt auch bei der Zwischenlagerung in Räumen, die nicht ohne weiteres öffentlich zugänglich sind.

- Ein getrenntes Sammeln von Datenträgern mit schutzwürdigem und nicht schutzwürdigem Inhalt hat sich in der Praxis nicht bewährt. Zu groß ist die Gefahr, daß Datenträger versehentlich falsch zugeordnet werden bzw. in den falschen Sammelbehälter gelangen.

- Das angeordnete Entsorgungsverfahren muß in regelmäßigen Abständen – und sei es nur stichprobenartig – z.B. durch den behördlichen Datenschutzbeauftragten auf seine Einhaltung und Wirksamkeit überprüft werden, ggf. sind entsprechende Anpassungen vorzunehmen.

Die Stadt Frankfurt am Main hat zwischenzeitlich verschiedene organisatorische und informatorische Maßnahmen ergriffen und mir diese schriftlich erläutert. Insbesondere wurde die Entsorgung des Büroabfalls neu geregelt, die Amtsleiter und sonstigen dienstlichen Vorgesetzten auf ihre Pflichten hingewiesen und die Mitarbeiter belehrt. Auch sollen weitere Geräte zur Aktenvernichtung beschafft werden.

Die Wirksamkeit dieser Maßnahmen wird Gegenstand einer erneuten Prüfung durch meine Mitarbeiter sein. Die mir übergebenen Unterlagen sind, soweit meine Zuständigkeit gegeben war, nach Prüfung des jeweiligen Sachverhalts von mir ordnungsgemäß vernichtet worden. Andere, aus dem Bereich nichtöffentlicher Stellen stammende Vorgänge, habe ich der nach dem Bundesdatenschutzgesetz zuständigen Aufsichtbehörde zur Klärung weitergereicht.

15.4
Viren

Eine besorgniserregende Entwicklung ist das vermehrte Auftreten sogenannter Programm-Viren. Diese Bezeichnung wird fälschlich auch undifferenziert für Programme benutzt, die den ordnungsgemäßen Betrieb einer DV-Anlage behindern oder gar unmöglich machen. Der als „Virus" bezeichnete Typ ist jedoch ein Spezialfall.

Für den Betreiber einer DV-Anlage ist es zumindest lästig, wenn durch ein eingeschleustes Virus-Programm das Betriebssystem außer Funktion gesetzt wird, d.h. abstürzt. Es trägt auch nicht zum ordnungsgemäßen Betrieb der Anlage bei, wenn auf dem Bildschirm der Sachbearbeiter plötzlich die Zeichen anfangen zu tanzen, der Eindruck eines Schneesturms entsteht oder ein Weihnachtsbaum mit dem fröhlichen Wunsch „merry christmas" erscheint. Das eigentliche Problem aus der Sicht des Datenschutzes liegt darin begründet, daß Daten durch Virus-Programme unbemerkt zerstört bzw. verändert werden können oder unberechtigte Zugriffe auf geschützte Daten und Programme möglich sind.

Bisher sind Virus-Programme hauptsächlich im Zusammenhang mit sogenannten „Hackern" im Bereich öffentlich zugänglicher DV-Netze oder auf privaten Personalcomputern aufgetaucht. Die Hessische Zentrale für Datenverarbeitung wurde jetzt erstmals mit dem Fall einer Virusverseuchung bei einem hessischen Landesamt konfrontiert.

Die dort eingesetzten PC's waren plötzlich nicht mehr in Betrieb zu nehmen. Da die Verfahrensanwender einen technischen Defekt der Geräte vermuteten, schalteten sie den Hersteller ein. Dieser stellte schnell fest, daß sich auf den Festplatten der PC's ein Virus vom Typ „Vienna 19" befand. Durch die Verwendung eines besonderen Programms zur Erkennung und Beseitigung von Programm-Viren und das Laden einer unverseuchten Sicherungskopie konnten die Rechner wieder in Betrieb genommen werden. Schaden war glücklicherweise nicht entstanden.

Die betroffene Stelle versuchte die Herkunft der Virus-Programme zu ermitteln. Den Verdacht, sie seien mit von der HZD beschaffter Software eingeschleust worden, konnte diese – allerdings mit großem Aufwand – widerlegen. Sie untersuchte zu diesem Zweck alle in der HZD vorhandenen PC's, die mit der betreffenden Software gearbeitet hatten, auf einen Virusbefall. Es stellte sich dabei heraus, daß keiner dieser Rechner „verseucht" war. Der Anwender stellte fest, daß zum Zeitpunkt der Verseuchung der PC's kein anderes Programm offiziell auf diese kopiert worden war. Es bleibt somit nur der Verdacht, daß ein Mitarbeiter einen PC der Dienststelle mit privaten Programmen zu privaten Zwecken genutzt haben muß und dabei ein verseuchtes Programm einschleppte.

Vorfälle dieser Art müssen unbedingt verhindert oder zumindest erschwert werden. Ich verweise in diesem Zusammenhang nochmals auf meine Ausführungen zur Datenverarbeitung mit PC (vgl. 15. Tätigkeitsbericht, Ziff. 9.3) und empfehle, die Verwendung privater Programme auf dienstlichen PC's in jedem Fall zu verbieten.

Die HZD hat aus diesem Vorfall die notwendige Konsequenz gezogen und ein Konzept in Auftrag gegeben, das die Weitergabe von Viren mit größtmöglicher Sicherheit ausschließt. Wesentliche Grundsätze dieses Konzeptes, an dem z.Z. gearbeitet wird, sind:

- Die Verwendung nicht dienstlich beschaffter Programme ist verboten.
- Dienstliche PC's dürfen nicht für private Zwecke genutzt werden.
- Es dürfen nur solche Datenträger verwendet werden, die von der HZD ausgegeben wurden (ausgenommen ist der Datenträgeraustausch im Rahmen von DV-Projekten, hierfür gelten Sonderregelungen).
- Alle Programme, die an Kunden ausgeliefert werden, müssen von einem nur für diesen Zweck vorgesehenen PC auf Disketten kopiert werden. Dieser PC ist mit einem Spezialprogramm versehen, das Viren erkennt und zum größten Teil auch eliminiert.
- Im Datenträgeraustausch angelieferte oder neu gekaufte Programme werden auf einem nur für diesen Zweck vorgesehenen „Quarantäne-PC" mit Spezialprogrammen untersucht, ehe sie verwendet werden. Die Originaldisketten müssen schreibgeschützt sein, wenn die Programme eingelesen werden.

15.5
Benutzerkontrolle bei DV-Anwendungen: Probleme der Passwortverwaltung

Ein Mitarbeiter der Stadt Neu-Isenburg war zuvor bei einer anderen Gemeinde beschäftigt und nutzte dort im Rahmen seiner Aufgaben ein DV-Verfahren, das auf dem Rechner des Kommunalen Gebietsrechenzentrums Frankfurt lief. Ihm war neben einer Benutzerkennung mit Passwort zur Anmeldung am Rechner ein Passwort zugewiesen worden, das ihn berechtigte, das DV-Verfahren aufzurufen. An dieses sogenannte Verfahrenspasswort waren die Berechtigungen gekoppelt, auf die Daten seiner Behörde zuzugreifen. Als er zur Stadt Neu-Isenburg wechselte, die bei demselben Gebietsrechenzentrum dasselbe DV-Verfahren nutzte, erhielt er auch hier wieder eine Benutzerkennung mit Passwort und ein Verfahrenspasswort. Nachdem er sich mit seiner neuen Benutzerkennung und Passwort am Rechner angemeldet hatte, probierte er sein altes Verfahrenspasswort aus. Er konnte sich nicht nur in dem Verfahren anmelden, sondern sogar in die Daten seiner vorherigen Dienststelle Einsicht nehmen. Von dem Bediensteten auf diese Schwachstelle hingewiesen, bat mich das KGRZ um Stellungnahme. Der Fall hat mich veranlaßt, die Anforderungen an eine effektive Benutzerkontrolle zu präzisieren.

15.5.1
Dokumentation von Verfahrenspasswörtern

In dem dargestellten Fall war im nachhinein nicht mehr feststellbar, an welcher Stelle es versäumt worden war, die nötigen Anweisungen zur Löschung des Verfahrenspasswortes zu geben. Für die Behörde und das Rechenzentrum stellte sich aber die Frage, wie zukünftig sicherzustellen ist, daß ein Verfahrenspasswort in dringenden Fällen, beispielsweise bei Krankheit oder Kündigung eines Mitarbeiters, gelöscht werden kann, wenn dieser nicht zu erreichen ist.

Die naheliegendste Lösung wäre, wenn entweder das Rechenzentrum oder die Behörde dokumentieren würde, welchem Benutzer welches Verfahrenspasswort zugewiesen wurde. Dies stünde aber im Widerspruch zu dem für die Dokumentation von Passworten geltenden Grundsatz, daß nur der einzelne Benutzer sein Passwort kennen darf und das Passwort grundsätzlich nicht schriftlich hinterlegt werden darf.

Diese Forderung scheint im vorliegenden Fall auf den ersten Blick unsinnig zu sein, da sie es dem Betreiber nur mit großem Aufwand ermöglicht, ohne die Hilfe des einzelnen Benutzers diesen von der Nutzung auszuschließen. Dieser Widerspruch löst sich jedoch auf, wenn man sich vor Augen hält, welche Funktionen ein Passwort hat und welche einer Benutzerkennung bzw. „User-Id" zugeordnet werden. Zur Anschauung bietet es sich an, den Anmeldevorgang an ein DV-System zu betrachten. Die Anmeldung an ein System sollte grundsätzlich in zwei Phasen erfolgen:

Identifikation
Die Identifikation gegenüber einem DV-System erfolgt durch die Eingabe einer Benutzerkennung bzw. „User-Id". Die Prüfung der Zugriffsrechte von Benutzern basiert immer auf einer Benutzerkennung und den ihr zugeordneten Rechten. Diese Rechte besagen beispielsweise, ob die Benutzerkennung Zugriff auf Dateien, Programme und andere Objekte hat. Auch in Protokollen wird auf diese Benutzerkennung Bezug genommen. Deshalb muß sie eindeutig einer Person zugeordnet sein. Um die Rechte von Benutzern verwalten zu können, muß dokumentiert sein, welche Person unter welcher Benutzerkennung arbeitet. Das gleiche gilt in Einzelfällen, wenn Protokolle gezielt ausgewertet werden müssen.

Authentifikation
Mit der Authentifikation wird bewiesen, daß sich tatsächlich die Person anmeldet, der eine bestimmte Benutzerkennung zugeordnet wurde. Obwohl zur Zeit neue Mittel zur Authentifikation aufkommen (Chipkarten, Fingerabdruckerkennung oder andere biometrische Verfahren), ist die Eingabe eines Passwortes die zur Zeit gebräuchlichste Methode. Der Gebrauch von Passworten ergibt nur Sinn, wenn ausschließlich der Benutzer sein Passwort kennt. Anderenfalls ist eine sichere Identifizierung mittels der Benutzerkennung nicht gegeben. Es darf daher nicht dokumentiert sein, welches Passwort ein Benutzer hat. Da es grundsätzliche Probleme gibt, ein Passwort geheim zu halten, muß durch verschiedene Maßnahmen versucht werden, dieses weitgehend sicherzustellen (siehe unter Ziff. 15.5.4).

Wenn die Begriffe „Benutzerkennung" und „Passwort" in der definierten Weise benutzt werden, handelt es sich im beschriebenen Fall bei dem „Verfahrens"passwort nicht um ein Passwort, sondern eher um eine Benutzerkennung. Da aber die Anmeldephasen nicht streng getrennt wurden, mußte schon bei der Identifikation versucht werden, zugleich die Authentifikation sicherzustellen. Dies ist eine prinzipielle Schwachstelle des angewandten Anmeldeverfahrens. Es muß einerseits der Person, die die Zugriffsrechte einträgt, bekannt sein, welchem Benutzer das Verfahrenspasswort zugeordnet ist, andererseits darf nur der Benutzer selbst sein Verfahrenspasswort kennen. In diesem speziellen Fall habe ich folgende pragmatische Lösung akzeptiert:

- Die speichernde Stelle (Behörde) oder das Rechenzentrum dokumentieren, welcher Benutzer mit welchem Verfahrenspasswort arbeitet. Es wird sichergestellt, daß ein Mißbrauch dieser Aufzeichnungen ausgeschlossen wird.

Um den Mißbrauch auszuschließen, wird insbesondere festgelegt:

- Die Stelle, die die Verwaltung der Verfahrenspassworte vornimmt, muß ihre Unterlagen sicher verschlossen aufbewahren.
- Der Personenkreis mit einem Zugriff auf diese Unterlagen wird so klein wie möglich gehalten.
- Die Benutzer haben ihre Verfahrenspassworte genauso zu behandeln, wie normale Passworte.

Gleichzeitig habe ich gefordert, daß die Anmeldeprozedur an das DV-Verfahren abgeändert wird.

15.5.2
Nutzung von Standardfunktionen

15.5.2.1
Begriffe

Um einen Rechner nutzen zu können, benötigt ein Anwender neben seinen Anwendungsprogrammen verschiedene andere Programme. Im Zusammenhang mit Standardfunktionen zur Sicherstellung des Datenschutzes sind dies vor allem

- das Betriebssystem
  Hierbei handelt es sich um die Programme, die für den Betrieb des Rechners unbedingt erforderlich sind. Das Betriebssystem verwaltet die Hardware und stellt sie den verschiedenen anderen Programmen zur Verfügung.

- TP-Monitor
  Ein TP-Monitor ist ein Spezialprogramm, welches den Ablauf von Programmen steuert. Es koordiniert auch den Zugriff mehrerer Programme auf die gleiche Datei und den Nachrichtenaustausch zwischen den Datenstationen und den anderen am Rechner angeschlossenen Geräten. Die Programme werden dabei durch Benutzer gestartet, die sich hierzu an dem TP-Monitor anmelden.

- Datenbankmanagementsystem
  Ein Datenbankmanagementsystem ist ein Paket von Spezialprogrammen, das Datenbestände verwaltet. Um auf die Datenbestände zugreifen zu können, muß in einem Anwendungsprogramm nicht mehr bekannt sein, wie die Daten auf dem DV-System genau gespeichert sind. Es wird lediglich eine Anfrage an das Datenbankmanagementsystem gerichtet und dieses stellt die Daten zur Verfügung.

15.5.2.2
Nutzung von Standardfunktionen

Alle technischen Sicherheitsfunktionen lassen sich den Gruppen

- Identifikation/Authentifikation

- regelbasierter Zugriffsschutz

- benutzerdefinierbarer Zugriffsschutz

- Protokollierung

zuordnen. Die neueren auf dem Markt befindlichen Betriebssysteme, TP-Monitore oder Datenbankmanagementsysteme haben standardmäßig Sicherheitsfunktionen eingebaut oder können mit Zusatzprodukten erweitert werden, die diese beinhalten. Man kann davon ausgehen, daß diese Produkte in der Regel die Sicherheitsfunktionen besser erfüllen, als wenn diese in einer Anwendung besonders programmiert wurden. Dies gilt insbesondere, wenn das Produkt durch das Bundesamt für die Sicherheit in der Informationsverarbeitung (BSI) zertifiziert wurde und eine ausreichende Qualitätsstufe gegeben ist.

Es sind daher vorrangig die mit dem Betriebssystem, TP-Monitor- und Datenbankmanagementsystem vorhandenen Sicherheitsfunktionen so weitgehend wie möglich zu nutzen. Erst wenn es nicht möglich ist, diese Standardfunktionen einzusetzen, sollten in einer Anwendung eigene Sicherheitsfunktionen programmiert werden.

15.5.3
Gestaltung von Anmeldeprozeduren

Ein wichtiges Sicherheitskriterium ist, daß sich ein Benutzer, der mit einem DV-Verfahren arbeiten will, identifizieren muß und eine Authentifikation verlangt wird. Es ist dabei nicht erforderlich, daß die Prüfung in dem Verfahren selbst vorgenommen wird. Es kann durchaus das Ergebnis einer vorhergehenden Benutzerkontrolle übernommen werden. In dem Ausgangsfall ist das nicht geschehen. Dort mußte sich der Mitarbeiter zwar mit einer Benutzerkennung und einem Passwort anmelden, es wurde dann aber die geprüfte Benutzerkennung im Verfahren nicht genutzt, um das Verfahrenspasswort oder den Zugriff zu kontrollieren.

Wenn diese Prüfungen im Verfahren vorgenommen werden, ist der Anmeldevorgang in die beiden Phasen Identifikation und Authentifikation zu trennen. Es ist dann möglich, die Verwaltung der an eine Benutzerkennung gekoppelten Berechtigungen und die Sperrung einer Benutzerkennung unabhängig von der Kenntnis des Passwortes vorzunehmen. Dies erleichtert letztlich auch die Dokumentation.

15.5.4
Forderungen an die technische Realisierung einer Passwortverwaltung

Um die prinzipiellen Schwachstellen weitestgehend auszuschließen, die die Nutzung von Passworten zur Authentifikation mit sich bringt, sind bei der technischen Realisierung einer Passwortverwaltung folgende Anforderungen zu berücksichtigen:

- Die Passworte sind verschlüsselt zu speichern; dabei ist eine Einwegverschlüsselung zu bevorzugen.

- Die Datei in der die Passworte gespeichert sind, sollte nicht anzeigbar sein.

- Der Benutzer muß sein Passwort ändern können.

- Ein Passwortwechsel muß in bestimmten Zeitabständen erzwungen werden, dabei hat sich eine Gültigkeitsdauer von maximal einem Monat bewährt.

- Es muß eine Mindestlänge der Passworte von 6 Stellen gegeben sein, wobei eine Länge von 8 Stellen anzustreben ist.

- Es sollte die Möglichkeit bestehen, bestimmte Passworte abzuweisen. Neben den zeitlich letzten 5 Passworten könnten auch Vornamen, Ortsnamen, Tastenkombinationen wie „123456" oder „qwertz" und andere triviale Begriffe dazugehören.

- Es muß der Zwang zur Passworteingabe bestehen, wenn eine Anmeldung erfolgt.

- Bei der Eingabe darf ein Passwort am Bildschirm nicht angezeigt werden. Es sollte sogar nicht möglich sein, die Länge des Passwortes zu erkennen.

- Die Fehlermeldung bei einer Anmeldung muß allgemein gehalten sein. Es darf nicht daraus hervorgehen, ob die Benutzerkennung oder das Passwort falsch eingegeben wurde.

- Es muß die Möglichkeit geben, eine Benutzerkennung automatisch zu sperren, wenn eine vorzugebende Anzahl ungültiger Passworteingaben erfolgt ist.

- Wird durch den Administrator ein Passwort für einen Benutzer vergeben, so darf dieses Passwort nur für einen Anmeldevorgang gültig sein. Es muß dann durch den Benutzer bei der ersten Anmeldung geändert werden.

15.5.5
Dokumentation von Passworten

Im Zusammenhang mit der Dokumentation von Passworten gilt folgender Grundsatz: Ein Benutzer muß sein Passwort gegenüber anderen Personen geheimhalten. Es darf folglich nicht so dokumentiert werden, daß andere Personen einen Zugriff darauf haben.

Obwohl diese Forderung für alle Benutzer Gültigkeit hat, ist eine Ausnahme denkbar: Wenn beispielsweise alle Personen in einem Rechenzentrumsbetrieb ausfallen, die die Datenschutzsoftware administrieren, ist eine ordnungsgemäße Datenverarbeitung nicht mehr möglich. Es können dann keine Benutzerkennungen angelegt oder gesperrt werden und es ist beispielsweise auch nicht möglich, Berechtigungen zu vergeben. Man kann sich sogar Fälle vorstellen, in denen der Betrieb für lange Zeit eingestellt werden muß, da auf Fehler nicht mehr reagiert werden kann. Um diese Gefahr möglichst gering zu halten, wäre es denkbar, die Funktion der Administration vielen Benutzern zu geben. Dieser Ansatz ist jedoch verfehlt, da der Kreis der Benutzer mit dieser Funktion so klein wie möglich zu halten ist. Eine Möglichkeit wäre aber z.B. eine Benutzerkennung mit Passwort zu dokumentieren, die die Berechtigung zur Administration der Schutzsoftware besitzt.

Diese Lösung, zu bestimmten Funktionen für Notfälle eine Benutzerkennung mit Passwort zu dokumentieren, ist in jedem Fall restriktiv zu handhaben. Sie ist nur zu verantworten, wenn auf dem DV-System kein weiterer Benutzer (in einer anderen Funktion) vorhanden ist, der die nötigen Berechtigungen für die ausgefallene Funktion vergeben kann. Beispiele für solche Funktionen sind die ACF2-Administration (Access Control Facility, vgl. hierzu auch 16. Tätigkeitsbericht, Ziff. 4.2.1) oder der Superuser auf UNIX-Systemen.

Wenn ein derartiger „Notuser" angelegt wird, müssen die Art der Aufbewahrung und die Nutzung sorgfältig geregelt werden. Dabei kann man sich an dem Umgang mit Betriebsgeheimnissen oder den Vorschriften für den Umgang mit VS-Sachen der Stufe VS-Vertraulich und höher orientieren. Wenn mit diesem „Notuser" gearbeitet wurde, ist umgehend eine dafür vorgesehene Instanz zu informieren. Ferner ist die benutzte „Notuser"-Id zu löschen und eine neue anzulegen.

16. Bilanz

16.1
Zusammenlegung von Meldeamt und Ausländerbehörde
(18. Tätigkeitsbericht, Ziff. 2.5)

Die Stadt Rüsselsheim hat sich zu meiner Kritik an der Zusammenlegung von Meldeamt und Ausländerbehörde bisher nicht abschließend geäußert, obgleich ich mehrfach eine Stellungnahme angemahnt habe.

16.2
Sicherheitsbehörden

16.2.1
Aufhebung der Grenzkontrollen zwischen einigen EG-Ländern – Zusatzübereinkommen zum Schengener Abkommen
(18. Tätigkeitsbericht, Ziff. 3.1, 17. Tätigkeitsbericht, Ziff. 1.3)

Nach dem von den Regierungen der fünf EG-Länder Bundesrepublik Deutschland, Frankreich, den Niederlanden, Belgien und Luxemburg im Jahre 1985 unterzeichneten „Schengener Abkommen" (GMBl. 1986, S. 79) hätte bereits am 1. Januar 1990 jegliche Grenzkontrolle zwischen den beteiligten Staaten fallen müssen. Zwei Gründe führten dazu, daß dies schließlich nicht geschah: Zum einen hatten die betroffenen Länder beschlossen, die aus Sicht der Sicherheitsbehörden für den Wegfall der Grenzkontrollen notwendigen kompensatorischen Maßnahmen in einem Zusatzübereinkommen festzulegen, dessen Fassung erst Ende 1989 fertiggestellt werden konnte. Zum anderen führte die Entwicklung in der ehemaligen DDR nach dem 9. November 1989 und die damit verbundene und zunächst ungelöste Frage einer Einbeziehung dieses Gebiets in den Schengener Verbund dazu, daß auf Initiative einzelner Bundestagsabgeordneter und dann auch der Bundesregierung mit den Partnerstaaten nachverhandelt werden mußte. Am 19. Juni 1990 haben die Regierungen der beteiligten Staaten das Zusatzübereinkommen unterzeichnet. Freilich ist es damit noch nicht unmittelbar in Kraft getreten, da es der Zustimmung durch die Parlamente der einzelnen Länder bedarf. In der Sache wurde es durch eine Protokollnotiz ergänzt, wonach sich infolge der Vereinigung der beiden deutschen Staaten die völkerrechtliche Bindungswirkung des Übereinkommens auch auf das Gebiet der früheren Deutschen Demokratischen Republik erstreckt.

In meinem letzten Tätigkeitsbericht habe ich im Hinblick auf den Entwurf des Zusatzübereinkommens einige Punkte kritisiert, die die Hessische Landesregierung dazu veranlaßten, beim Bundesminister des Innern eine Stellungnahme einzuholen. Dessen Äußerungen hat die Landesregierung in ihrer Stellungnahme zu meinem 18. Tätigkeitsbericht (Drucks. 12/7182) abgedruckt. Der Bundesinnenminister teilt meine Ansicht nicht, daß das Zusatzübereinkommen und die mit ihm verbundene Verarbeitung von Fahndungsdaten (Fahndungsdatenverbund), von Daten über Asylantragsteller und Ausländer insbesondere aus Drittstaaten außerhalb des Kreises der Schengener Partner in ein europäisches Datenschutzkonzept als Grundlage für die polizeiliche Zusammenarbeit eingefügt werden müssen. Vielmehr hält er die Datenschutzregelungen, die auf Betreiben der Datenschutzbeauftragten der beteiligten Länder in das Zusatzübereinkommen aufgenommen wurden, für ausreichend. Ebensowenig sieht er die Notwendigkeit bereichsspezifischer Datenschutzbestimmungen für Strafprozeßordnung und Polizeigesetze. Nach seiner Auffassung reicht die bisherige Regelung durch Verwaltungsvorschriften aus. Dies widerspricht jedoch den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil 1983 formuliert hat. Danach sind bereichsspezifische Regelungen für diese Fachgebiete unabdingbar.

Mittlerweile hat die EG-Kommission den Entwurf einer Richtlinie vorgelegt, mit der die Mitgliedsstaaten der Gemeinschaft zur Schaffung von Datenschutzbestimmungen verpflichtet werden sollen (vgl. Ziff. 2 dieses Berichts). Soweit bisher nationales Datenschutzrecht noch nicht vorhanden ist, müßte diese Richtlinie jedoch noch umgesetzt werden. Für das Problem der polizeilichen Datenverarbeitung wird die Richtlinie, da sie ganz allgemein den öffentlichen und den privaten Sektor anspricht, praktisch keine Vorgaben enthalten. Es bleibt somit bei der im Schengener Zusatzübereinkommen bekräftigten Verpflichtung, die Empfehlung des Ministerkomitees des Europarats vom 17. September 1987 (Nr. R (87) 15) an seine Mitgliedsstaaten, „über die Nutzung personenbezogener Daten im Polizeibereich" in konkrete Regelungen umzusetzen.

Sicherlich, das Zusatzübereinkommen enthält, bezogen auf die unmittelbar auf ihm aufbauende personenbezogene Datenverarbeitung eine Reihe von Datenschutzbestimmungen, die insbesondere für das sog. Schengener Informationssystem – dem automatisierten Verbund der Fahndungsdatenbestände aller beteiligter Länder – eine Vielzahl von Schutzmechanismen vorsehen. Damit ist aber immer noch nicht geklärt, was mit den einzelnen Daten, die von einer Polizeidienststelle eines Landes an die eines anderen Landes übermittelt worden sind, geschehen darf. Immer noch verfügen einzelne Länder, wie Belgien und Luxemburg, aber auch Italien, das soeben dem Schengener Abkommen beigetreten ist, nicht über die entsprechenden Datenschutzvorschriften. Gleiches gilt für die weiteren Anwärter Spanien und Portugal.

Positiv ist zu vermerken, daß auch das Bundesinnenministerium – wie von mir gefordert – für die Verarbeitung von Ausländerdaten im Rahmen des Schengener Übereinkommens die Schaffung präziser Datenschutzregelungen aller Schengener Vertragsstaaten für erforderlich hält.

Erfreulich ist außerdem, daß die nun im Juni 1990 unterzeichnete Fassung einige datenschutzrechtliche Verbesserungen enthält. So wurde entgegen der noch in der Stellungnahme des Bundesministers des Innern vertretenen Ansicht, die Schengener Zusammenarbeit müsse sich auch auf alle Aufgabengebiete des Verfassungsschutzes bzw. der Nachrichtendienste erstrecken, die früher im Entwurf enthaltene Klausel gestrichen, nach der die „nationalen Sicherheitsdienste" am Informationsaustausch teilhaben sollten.

Eine Verbesserung bedeuten auch die in einem besonderen Kapitel VI „Datenschutz" des Zusatzübereinkommens zusammengefaßten Bestimmungen. Danach verpflichtet sich jede Vertragspartei, spätestens bis zum Inkrafttreten des Zusatzübereinkommens in ihrem nationalen Recht wenigstens für die automatisierte Verarbeitung personenbezo-

gener Daten, die nach diesem Übereinkommen übermittelt werden, die erforderlichen Maßnahmen zur Gewährleistung eines einheitlichen Datenschutzstandards zu schaffen. Maßstäbe hierfür sind die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981. Erst dann, wenn diese Regelungen in allen Ländern in Kraft getreten sind, dürfen Übermittlungen nach dem Übereinkommen beginnen. Darüber hinaus enthält das Kapitel Regelungen zur Zweckbindung, Dokumentationspflichten und eine Verpflichtung zur Schaffung einer nationalen Datenschutzkontrollinstanz zur Überwachung der Datenverarbeitung nach dem Abkommen. Die Datenschutzregelungen des Zusatzübereinkommens beziehen sich nicht nur auf den automatisierten, sondern auch auf den nicht automatisierten Gebrauch personenbezogener Informationen.

Ergänzt um die besonderen Bestimmungen für den Datenschutz und die Datensicherung zum sog. Schengener Informationssystem (dem automatisierten Fahnungsverbund) bilden diese Vorschriften einen brauchbaren datenschutzrechtlichen Rahmen, um eine Handhabung zu gewährleisten, die dem Recht auf informationelle Selbstbestimmung aller betroffenen Bürger Rechnung trägt. Andere, noch recht unbestimmte Vorschriften, etwa über die allgemeine polizeiliche Zusammenarbeit, orientieren sich hingegen an dem auf dieser Grundlage in den meisten Partnerstaaten noch zu schaffenden nationalen Datenschutzrecht. Es wird Aufgabe der beteiligten Datenschutzinstanzen sein, den Gesetzgebungsprozeß in den betroffenen Ländern genau zu beobachten und ihren Einfluß geltend zu machen, daß die zu erlassenden Bestimmungen keine unverhältnismäßige Einschränkung des Rechts auf informationelle Selbstbestimmung vorsehen.

16.2.2
Die Datei ADOS der Verfassungsschutzämter
(18. Tätigkeitsbericht, Ziff. 5.2)

Im letzten Tätigkeitsbericht habe ich die gemeinsam vom Bundesamt für Verfassungsschutz und den Landesämtern betriebene Datei ADOS („Adressen- und Objektedatei Ost") kritisiert und deren Löschung gefordert.

Im November 1989 teilte mir das Hessische Innenministerium mit, daß das Landesamt für Verfassungsschutz Hessen künftig keine Daten mehr über Aus- und Übersiedler in die Datei einstellen würde. Das Schicksal der bestehenden Datensammlung erschien dagegen längere Zeit ungewiß. Immerhin ging es dabei um mehr als 100.000 Datensätze von gänzlich unverdächtigen Personen. Nicht zuletzt aufgrund der Kritik der Datenschutzbeauftragten fiel dann endlich im März 1990 die Entscheidung, daß der gesamte ADOS- Datenbestand gelöscht wird. Die Arbeitsgemeinschaft der Innenministerien stellte dazu am 5. März 1990 fest, „daß angesichts der politischen Entwicklung in der DDR und in Osteuropa die Notwendigkeit der Datei ADOS jetzt nicht mehr gegeben (sei)" und beschloß, „die gespeicherten Daten zu löschen und die dazu noch vorhandenen Unterlagen zu vernichten".

16.3
Ausländerzentralregister
(18. Tätigkeitsbericht, Ziff. 8)

Im letzten Tätigkeitsbericht habe ich den von der Bundesregierung vorgelegten Entwurf für ein Ausländerzentralregistergesetz (Bundestag-Drucks. 11/5828) kritisiert. Der Entwurf wurde gemeinsam mit dem Entwurf für ein Gesetz zur Neuregelung des Ausländerrechts am 9. Februar 1990 im Bundestag beraten und an die Ausschüsse überwiesen, aber im Gegensatz zu diesem nicht verabschiedet.

Die Datenverarbeitung in dem beim Bundesverwaltungsamt in Köln geführten Ausländerzentralregister erfolgt somit nach wie vor ohne gesetzliche Grundlage. Völlig unannehmbar ist, daß unter dieser Voraussetzung der Ausbau der Datenverarbeitung im Ausländerzentralregister auch noch weiter voran getrieben wird. Ein vom Bundesverwaltungsamt erarbeitetes neues Datenverarbeitungssystem soll in Kürze in Betrieb genommen werden. Vorgesehen ist dabei u.a. die Installierung von Online-Anschlüssen vorerst für die Ausländerbehörden, die damit die Möglichkeit erhalten, regelmäßig sowohl Daten direkt in das Register einzugeben, als auch abzurufen.

16.4
Personaldatenverarbeitung

16.4.1
Hessisches Personalinformationssystem – HEPIS
(16. Tätigkeitsbericht, Ziff. 8.2.2)

Die beim Landespersonalamt geführte HEPIS-Datei kann seit der Novellierung des HDSG zum 1. Januar 1987 nicht mehr gleichzeitig für Zwecke der Planung und des Verwaltungsvollzuges genutzt werden. Eine umfassende Nutzung von HEPIS erfordert eine spezifische Rechtsgrundlage. Dieser Auffassung ist auch der Unterausschuß Personalwesen des Landesautomationsausschusses. Bis heute liegt jedoch eine solche Regelung nicht vor.

Ich habe daher den gegenwärtigen Umfang der Verwendung von HEPIS gemäß § 27 HDSG beanstandet und verlangt, bis zum 1. September 1990 die Datensätze entsprechend den Anforderungen des § 32 Abs. 2 Satz 2 HDSG zu anonymisieren oder zu löschen. Eine Veränderung der archivierten Datensätze ist inzwischen erfolgt: Die Merkmale Name, Adresse, Tag und Monat des Geburtsdatums und der numerische Teil der Personalnummer wurden gelöscht.

Zur fehlenden Rechtsgrundlage teilte das Landespersonalamt lediglich mit, es sei weiterhin beabsichtigt, eine solche in einem Artikelgesetz zur Landesstatistik noch in dieser Legislaturperiode vorzulegen. Diese Absicht rechtfertigt jedoch nicht, in der bisherigen Weise mit der Datei weiterzuarbeiten.

16.4.2
Unzulässiger Umgang mit Personalakten
(18. Tätigkeitsbericht, Ziff. 9.1.2)

Der letzte Tätigkeitsbericht schilderte den Fall eines Schulleiters, der Personalnebenakten der Lehrer in seine Wohnung mitgenommen hatte, sie dort zunächst vergaß und Wochen später durch einen Rechtsanwalt an das Staatliche Schulamt zurückgab.

In seiner Stellungnahme auf meine Beanstandung sieht auch das Kultusministerium in dem Verhalten des Schulleiters einen erheblichen Verstoß gegen das Hessische Datenschutzgesetz. Das Ministerium teilte mir außerdem mit, es werde den Beamten entsprechend belehren und im Rahmen der Schulaufsicht darauf achten, daß derartige Verstöße in Zukunft unterbleiben.

16.4.3
Automatisierte Verarbeitung von Lehrerdaten
(18. Tätigkeitsbericht, Ziff. 9.1.3)

Das Kultusministerium hat das angekündigte Konzept für die zukünftige Gestaltung der „Verarbeitung von Lehrerdaten zu Planungszwecken" im Juni 1990 im Rahmen der „Neuorganisation der statistischen Erhebungen im Schulbereich" vorgelegt. Die Vorstellungen der vorbereitenden Projektgruppe wurden mehrmals mit mir beraten. Mit der nunmehr vorgesehenen Lehrerunterrichtsdatei (LUD), die die Lehrerindividualdatei (LID) ablöst, ist sichergestellt, daß eine Trennung von Planungs- und Verwaltungsdatenverarbeitung erfolgt (§ 34 Abs. 8 HDSG). Darüber hinaus werden die Datensätze in einer Form in die LUD aufgenommen, die einen unmittelbaren Personenbezug ausschließt (§ 32 Abs. 2 HDSG).

16.5
Post und Rundfunk

16.5.1
Neue Datenschutzverordnungen nach dem Poststrukturgesetz
(18. Tätigkeitsbericht, Ziff. 16.2.3.1)

Noch immer stehen die bereichsspezifischen Einzelheiten des Datenschutzes für Telekommunikationsnetze und -dienste nach der Änderung der Poststruktur am 01. Juli 1989 nicht fest. Die speziellen Verordnungen für die Deutsche Bundespost/TELEKOM sowie die privaten Netz- und Diensteanbieter, die nach dem Poststrukturgesetz von der Bundesregierung zu erlassen sind, lagen zum Jahresende 1990 noch nicht einmal im Entwurf vor. Dabei besteht erheblicher Zeitdruck, da die Telekommunikationsordnung (TKO), die für den öffentlich-rechtlichen TK-Bereich, also die DBP/TELEKOM, einen Grundstandard an Datenschutzbestimmungen enthält, Mitte 1991 außer Kraft tritt. Erst recht unbefriedigend ist das Schutzniveau im nicht-öffentlichen Bereich, für den die TKO nicht gilt; für die privaten TK-Unternehmen sind bis zum Erlaß der speziellen Datenschutzverordnung nur die allgemeinen Bestimmungen des Bundesdatenschutzgesetzes anwendbar.

Hinzu kommt, daß die öffentliche Diskussion über den Datenschutz im Fernmeldeverkehr sich im Jahr 1990 erheblich intensiviert hat. Kritisch gesehen werden insbesondere die mit dem neuen ISDN-Netz der Bundespost verbundenen Leistungsmerkmale Rufnummernanzeige, Anrufumleitung und Einzelgebührennachweis. Selbst die EG-Kommission hat hier bereits reagiert und detaillierte Regelungen in ihren „Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" vom 27. Juli 1990 aufgenommen (Bundesrats-Drucks. 690/90 vom 04.10.1990, s. dazu auch oben Ziff. 2.1).

Ich erwarte, daß die Bundesregierung sich in wesentlichen Punkten an den EG-Vorschlägen orientiert. Dies gilt beispielsweise für den persönlichkeitsrechtlichen Interessenausgleich zwischen dem anrufenden und dem angerufenen Teilnehmer bei der sog. „Rufnummernanzeige". Art. 12 des EG-Richtlinienentwurfs schreibt für dieses Leistungsmerkmal vor, daß der anwählende Teilnehmer mit einer einfachen technischen Einrichtung (z.B. Knopf) die Weiterleitung seiner Telefonnummer an den Gesprächspartner von Fall zu Fall unterbinden können muß. Umgekehrt ist dem angerufenen Teilnehmer die Möglichkeit zu schaffen, ankommende Verbindungen auf diejenigen zu beschränken, die durch Anzeige der Nummer identifiziert sind.

16.5.2
Kontrollbefugnis beim Hessischen Rundfunk
(18. Tätigkeitsbericht, Ziff. 18.11)

Die seit Inkrafttreten des dritten Hessischen Datenschutzgesetzes am 1. Januar 1987 bestehende Kontroverse mit dem Hessischen Rundfunk über Bestehen bzw. Umfang meiner Kontrollbefugnis konnte im April 1990 beigelegt werden.

Hilfreich war dabei die Vermittlungstätigkeit der Hessischen Staatskanzlei. In einem Briefwechsel zwischen dem Intendanten des Hessischen Rundfunks und mir wurden die Grundsätze und die künftige Verfahrensweise für die Beratungs- und Überwachungstätgkeit in bezug auf die Datenverarbeitung beim HR festgelegt.

Klargestellt wurde zum einen, daß ich die Beschreibung aller Dateien des HR erhalte, soweit sie dem nicht-journalistischen Bereich zuzuordnen sind. Diese Meldung zum Dateienregister ist inzwischen erfolgt. Vereinbart wurde weiter, daß nach förmlichen Überprüfungen, etwa Kontrollbesuchen, der Intendant und nach ihm – soweit erforderlich – die Aufsichtsgremien zu den Beanstandungen Stellung nehmen können; dies habe ich ohnehin immer für eine Selbstverständlichkeit gehalten. Im Tätigkeitsbericht werde ich auf Einzelheiten von Kontrollen nur dann eingehen, soweit Beanstandungen nicht vom Intendanten oder ggf. den Aufsichtsgremien Verwaltungsrat und Rundfunkrat ausgeräumt worden sind.

Mit dieser Absprache scheint mir ein tragbarer Kompromiß gefunden, der den Kern meiner Kontrollzuständigkeit nicht antastet, gleichzeitig aber ausreichend auf die Befürchtungen des Hessischen Rundfunks wegen der möglichen Gefährdung seiner Staatsfreiheit Rücksicht nimmt. Den Unterausschuß Informationsverarbeitung und Datenschutz des Hessischen Landtags habe ich über die getroffene Regelung im Juni 1990 unterrichtet.

16.6
Statistik

16.6.1
EG-Statistikverordnung
(18. Tätigkeitsbericht, Ziff. 3.2)

Die „Verordnung über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaft" – kurz: EG- Statistikverordnung – ist am 11. Juni 1990 verkündet worden und wenige Tage später in Kraft getreten (vgl. Amtsblatt der EG, Nr. L 151/1 vom 15.06.1990). Kleinere Verbesserungen konnten zwar noch erzielt werden; die Kernpunkte meiner im letzten Tätigkeitsbericht geäußerten Kritik sind jedoch nicht ausgeräumt worden. Dies gilt für die nach wie vor fehlenden Vorschriften über die frühzeitige Anonymisierung und die Datensicherungsvorkehrungen innerhalb des EG-Statistikamts ebenso wie für die Tatsache, daß ein aus Regierungsvertretern zusammengesetzter „Ausschuß für die statistische Geheimhaltung" eine unabhängige Datenschutzkontrolle nicht ersetzen kann.

Insgesamt ist nicht gewährleistet, daß das durch die deutschen Statistikgesetze in Bund und Ländern vorgeschriebene Datenschutzniveau in dem Europäischen Amt in Luxemburg gewahrt wird. Abzuwarten bleibt, welche Auswirkungen in diesem Zusammenhang die Erklärung der Kommission vom 18. Juli 1990 haben wird, in der sie sich dazu verpflichtet, die im Entwurf der Datenschutzrichtlinie (dazu Ziff. 2 dieses Berichts) enthaltenen Regelungen auf die Verarbeitung personenbezogener Daten in ihrem Zuständigkeitsbereich anzuwenden (vgl. Bundesrats-Drucks. 690/90 v. 04.10.90, S. 79).

16.6.2
Volkszählung 1987
(18. Tätigkeitsbericht, Ziff. 18.7)

16.6.2.1
HEPAS-NEU: Auswertung von Volkszählungsdaten

Mit dem Abschluß der Aufbereitung der Volkszählungsdaten im Hessischen Statistischen Landesamt (HSL) und der Veröffentlichung des bundeseinheitlichen Tabellenprogramms nehmen die Datenanforderungen der Kommunen beim HSL zu. Personenbeziehbare Einzelangaben aus der Volkszählung 1987 dürfen jedoch nur an die Gemeinden weitergegeben werden, die eine abgeschottete Statistikstelle haben (§ 14 Abs. 1 Volkszählungsgesetz; s. dazu 17. Tätigkeitsbericht, Ziff. 7.2.1).

Mittlerweile wollen auch die Kommunalen Gebietsrechenzentren (KGRZ) des DV-Verbundes Statistikdaten aus der Volkszählung 1987 den Gemeinden ihres Einzugsbereichs zur Nutzung anbieten. Nach Vorstellung der Kommunalen Gebietsrechenzentren soll sich dieses Angebot nicht auf die Städte mit separatem Statistikamt beschränken. Das Auswertungsprogramm im Rahmen des Verfahrens „HEPAS-NEU" soll den interessierten Anwendern die Möglichkeit eröffnen, VZ-Daten für eigene Zwecke abweichend von den Standardtabellen auswerten zu lassen.

Die Bereitstellung des Datenmaterials für die Kommunalen Gebietsrechenzentren durch das Hessische Statistische Landesamt könnte allerdings nur unter Berücksichtigung der in § 14 VZG formulierten Übermittlungsbedingungen stattfinden. Soweit die Kommunalen Gebietsrechenzentren als Auftragnehmer der Kommunen agieren, können sie nicht mehr Daten erhalten als der Auftraggeber, also die kommunale Gebietskörperschaft selbst. Dies schließt es aus, daß ein KGRZ gleichsam „auf Vorrat" personenbeziehbare Einzelangaben auch für Gemeinden ohne „abgeschottete" Statistikeinheit vorhält, auch wenn bei der Auswertung durch das KGRZ strikt darauf geachtet würde, daß die an die Kommune weitergegebenen Daten ausreichend aggregiert sind. Abgesehen von diesen Rechtsfragen wären bei

der Verarbeitung von VZ-Einzelangaben in den KGRZ für das HEPAS-NEU-Verfahren zusätzliche Vorkehrungen der Datensicherung zu treffen.

Mehrere Gespräche mit Vertretern der Kommunalen Gebietsrechenzentren über die Realisierbarkeit dieses Projekts haben 1990 stattgefunden. Das Hessische Statistische Landesamt hat inzwischen aus statistikrechtlichen Gründen die Bereitstellung des von den Kommunalen Gebietsrechenzentren gewünschten Datenmaterials abgelehnt.

16.6.2.2
Weitergabe von Volkszählungsdaten

Sollen kleinräumige statistische Ergebnisse weitergegeben werden, die personenbeziehbare Einzelangaben enthalten, muß eine Zusammenfassung mehrerer Blockseiten (kleinste Gliederungseinheit) zu höheren Einheiten erfolgen (§ 15 Abs. 4 Volkszählungsgesetz).

Das Statistische Landesamt stellt Dateninteressenten ohne privilegierten Status Angaben auf der Grundlage des bundeseinheitlichen Blockprogramms II zur Verfügung, das eine Vielfalt von VZ-Daten in vorher festgelegten Tabellenstrukturen ausweist. Zur Sicherung der Anonymität werden im Rahmen der maschinellen Auswertung auf der Ebene von Blöcken bzw. Blockseiten Feldbesetzungen, die nicht mindestens drei Fälle aufweisen, unterdrückt und am Ende in einem sogenannten Restblock zusammengefaßt. Unabhängig davon, daß m.E. diese von den Statistikern festgelegte Aggregation mitunter ungenügend sein kann, wird das Reidentifizierungsrisiko erhöht, wenn der Empfänger – wie in einem mir vorgelegten Fall ein privates Planungsinstitut – bei der Gemeinde zusätzlich die zur organisatorischen Vorbereitung der Volkszählung seinerzeit erstellten und dort teilweise noch vorhandenen Unterlagen anfordert, die die Feststellung der zu einer Blockseite gehörenden Anschriften ermöglichen (z.B. die sog. Gemeindeliste). Bei bestimmten Konstellationen wäre dann die Reidentifizierung eines Haushaltes und damit der darin lebenden Einzelpersonen möglich.

Das Bundesverfassungsgericht hat in seinem Volkzählungsurteil von 1983 gerade den Aspekt der möglichen Reidentifizierung thematisiert und geeignete gesetzliche und technische Maßnahmen gefordert, die dem entgegenwirken sollen. Konkretisiert sind diese Erfordernisse in § 15 Abs. 4 Satz 4 VZG.

Im konkreten Fall hat meine Intervention dazu geführt, daß die Gemeinde nicht die angeforderte präzise Blockseitenbeschreibung herausgab, sondern nur höher aggregierte räumliche Bezugsgrößen ohne Feststellbarkeit der Anschriften. Das Hessische Statistische Landesamt habe ich darauf hingewiesen, daß teilweise noch Kopien von Gemeindelisten bei Kommunalverwaltungen existieren, wie dies als Nachweis nach Ablieferung der Erhebungsunterlagen in Ziff. 3.3.4 der Gemeindeanleitung für die Durchführung der Volkszählung 1987 auch vorgesehen war. Diese Nachweisfunktion für die Vollzähligkeit aller Zählbezirke besteht längst nicht mehr, so daß die verbliebenen Gemeindelisten außerhalb von kommunalen Statistikstellen zu vernichten sind. Ich habe das HSL gebeten, dies den Gemeinden noch einmal ausdrücklich mitzuteilen.

16.6.3
Änderung des Mikrozensusgesetzes
(14. Tätigkeitsbericht, Ziff. 5.3.2)

Erhebungen über die Bevölkerung und den Arbeitsmarkt werden seit 1957 im Rahmen des sog. Mikrozensus auf Stichprobenbasis durchgeführt. Das Mikrozensusgesetz (MZG) vom 10. Juni 1985 war bis Ende 1990 befristet. Im 14. Tätigkeitsbericht hatte ich mich eingehend dazu geäußert.

Das am 1. Januar 1991 in Kraft getretene Änderungsgesetz (BGBl I/90, 2837) sieht die Verlängerung der Geltungsdauer des Mikrozensusgesetzes bis zum Jahr 1995 vor. Von inhaltlicher Bedeutung sind die Reduzierung des Erhebungsprogramms um die Fragen zur Wohnsituation sowie zu Urlaubs- und Erholungsreisen, der Wegfall der Testerhebungen und die Ausdehnung der freiwilligen Auskunftserteilung. Außerdem schließt die Neuregelung die Anwendung der Bußgeldvorschriften der §§ 23 und 24 des Bundesstatistikgesetzes (BStatG) aus. Damit wird auf das Mittel der Geldbuße bei Verletzung der Auskunftspflicht verzichtet.

Der Bundesrat hatte zum Regierungsentwurf kritisch Stellung genommen (Bundesrats-Drucks. 310/90 – Beschluß –). Vor allem der Wegfall des Bußgelds und der Fragen zur Wohnsituation fand keine Zustimmung. Die Bundesregierung hat in ihrer Gegenäußerung die Änderungswünsche des Bundesrates nicht berücksichtigt. Auch der federführende Innenausschuß des Deutschen Bundestages hat den Gesetzentwurf der Bundesregierung ohne Änderung angenommen. Daß die Änderungsvorschläge der Länder nicht akzeptiert wurden, hat wiederum zu Kritik in der abschließenden Beratung des Bundesrates geführt (vgl. Protokoll der 625. Sitzung vom 14.12.1990, S. 672 f.).

Positiv bewerte ich, daß das Gesetz – entgegen den Empfehlungen des Wissenschaftlichen Beirates für den Mikrozensus – den Befragten mehr Freiwilligkeit einräumt und die Bußgeldandrohung beseitigt. Eine Gesamtüberarbeitung der Mikrozensusgesetzgebung unter den Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts steht allerdings noch aus.

16.6.4
Hochschulstatistikgesetz
(18. Tätigkeitsbericht, Ziff. 10.2.2)

Der Bundestag hat am 19. September 1990 mit Zustimmung des Bundesrates das neue Hochschulstatistikgesetz verabschiedet (Bundesrats-Drucks. 624/90 und 440/90). Damit ist nach vielen vergeblichen Anläufen endlich eine verfassungskonforme Rechtsgrundlage für die Hochschulstatistik geschaffen worden. Wegen der notwendigen Umstellung sowohl für die Erhebungs- und Aufbereitungsprogramme als auch für das Erhebungsverfahren wird das Gesetz jedoch erst am 1. Juni 1992 in Kraft treten (BGBl. I 1990 S. 2414). Der im letzten Tätigkeitsbericht behandelte Regierungsentwurf (Bundestags-Drucks. 11/5832 und Bundesrats-Drucks. 416/89) hat allerdings noch einige Änderungen und auch datenschutzrechtliche Verbesserungen erfahren.

Entsprechend einer Empfehlung des Bundesrates ist auf die sechsjährliche Individualerhebung des wissenschaftlichen und künstlerischen Personals verzichtet worden. Statt dessen wird im Rahmen der jährlichen Personalstatistik eine differenziertere Verwaltungserhebung über das wissenschaftliche und künstlerische Hochschulpersonal durchgeführt.

Während im Regierungsentwurf ganz auf die Abiturientenbefragung verzichtet worden war, sieht das verabschiedete Gesetz nunmehr eine Befragung auf der Basis freiwilliger Beteiligung vor.

Der Regierungsentwurf erlaubte dem Statistischen Bundesamt die Durchführung von Zusatzaufbereitungen unabhängig davon, ob die Statistischen Landesämter diese durchführen oder nicht. Der Bundesrat sah darin einen unzulässigen Eingriff in die Zuständigkeit der Landesämter und berief sich auf Art. 83 ff Grundgesetz, wonach die Ausführung von Bundesgesetzen grundsätzlich Ländersache ist. Auf Vorschlag des Vermittlungsausschusses wurde die Vorschrift deshalb ersatzlos gestrichen.

Um eine mißbräuchliche Verwendung der Matrikelnummer bei der Studentenstatistik zu verhindern, wurde die im Regierungsentwurf enthaltete Vorschrift über Hilfsmerkmale ergänzt: Die Matrikelnummer muß nach Abschluß der Vollständigkeits- und Plausibilitätsprüfung gelöscht werden und darf nicht für einen Vergleich der Erhebungsmerkmale mit denjenigen aus der nachfolgenden Erhebung verwendet werden.

17. Materialien

17.1
20 Jahre Datenschutz in Hessen — eine kritische Bilanz.
(Rede des Hessischen Datenschutzbeauftragten Prof. Dr. S. Simitis in der Veranstaltung am 10. Oktober 1990 im Hessischen Landtag zum 20. Jahrestag der Verabschiedung des ersten Hessischen Datenschutzgesetzes)

Herr Präsident, meine Damen und Herren,
der 8. Juli 1970 war in der Geschichte des Hessischen Landtags, zumindest auf den ersten Blick, ein ganz normaler Sitzungstag. Je ein Dringlichkeitsantrag zur Finanzierung der Bremer Universität, zur Fürsorgepflicht des Landes für seine Beamten und zur Medizinischen Poliklinik der Universität Marburg, die übliche Fragestunde sowie die Lesung von siebzehn Gesetzen mit so verschiedenen Gegenständen wie etwa dem Schutz der Berufsbezeichnung „Ingenieur", der Kommunal- und Bauaufsicht des Innenministers über die Landeshauptstadt Wiesbaden, der Landeshaushaltsordnung, der Aufwandsentschädigung ehrenamtlicher Bürgermeister und dem Hessischen Investitionsfonds bestimmten die Tagesordnung. Alles in allem, parlamentarische Routine.

Spätestens als der amtierende Präsident, der Abgeordnete Dr. Großkopf, den Tagesordnungspunkt 8, „Erste Lesung des Entwurfs für ein Datenschutzgesetz", aufrief, mehrten sich freilich die Anzeichen dafür, daß der Hessische Landtag vor einer seiner wichtigsten Entscheidungen stand. Nicht etwa deshalb, weil die Debatte kontrovers oder gar stürmisch verlief; sie war im Gegenteil relativ kurz und weitgehend vom Konsens geprägt, eine Feststellung, die erst recht für die zweite und dritte Lesung am 30. September 1970 gilt. Auch nicht so sehr im Hinblick darauf, daß der damalige Ministerpräsident, Albert Osswald, den ich mich sehr freue heute hier zu sehen, selbst das Wort ergriff, um die Gesetzesvorlage zu begründen. Weit eher lassen die wiederholten Hinweise auf die Originalität, ja die Einmaligkeit der vorgeschlagenen Regelung aufhorchen. In den Worten des Ministerpräsidenten: ein Gesetzentwurf, für den es weder in der Bundesrepublik noch im Ausland eine Parallele gäbe und mit dessen Hilfe erstmals versucht würde, ich zitiere: „die möglichen Konsequenzen für Bürger und Staat aus dem Einsatz der elektronischen Datenverarbeitung offenzulegen und aufzufangen".

Genaugenommen reagierte die Landesregierung mit ihren Vorschlägen auf eine von ihr selbst Ende der sechziger Jahre eingeleitete und seither konsequent weiterverfolgte Entwicklung. Um noch einmal Ministerpräsident Osswald zu zitieren, diesmal aus seinem Vorwort zum „Großen Hessenplan"; Ich zitiere: „Regieren und Verwalten", sagte er, „wird in Zukunft mit der Entwicklung von Informationssystemen und Datenbanken untrennbar verbunden sein". Ende des Zitats. Die Akzente waren damit gesetzt. Für die Landesregierung gab es keinen Zweifel: Der systematische Ausbau einer konsequent integrierten Datenverarbeitung war aus ihrer Sicht die ebenso selbstverständliche wie unausweichliche Antwort auf den manifesten, vor allem durch eine unablässig expandierende Leistungsverwaltung dokumentierten strukturellen Wandel der staatlichen Tätigkeit. Nichts könne, so meinte man, die längst fällige

Rationalisierung, aber auch die unerläßliche Rationalität der öffentlichen Verwaltung so nachhaltig fördern, wenn nicht sogar garantieren, wie eine automationsgestützte Verarbeitung aller von der Administration benötigten Informationen.

Der Computer signalisiert, so gesehen, den Beginn eines neuen Zeitalters in dem sich, dank der Automatisierung des Informationsprozesses, nicht nur zum ersten Mal die Möglichkeit eröffnet, tradierten Prinzipien wie etwa den Geboten der Zweckmäßigkeit und Wirtschaftlichkeit besser denn je Rechnung zu tragen, vielmehr auch, jetzt zitiere ich wieder: „den Bedarf an Einrichtungen der sozialen, kulturellen und wirtschaftlichen Infrastruktur ... der voraussehbaren gesellschaftlichen Entwicklung anzupassen", Ende des Zitats, sowie sachlich, räumlich, zeitlich und finanziell aufeinander abzustimmen und schließlich Legislative und Exekutive in die Lage zu versetzen, ich zitiere wieder: „die zumeist intuitiven politischen Entscheidungen durch rationale Schlußfolgerungen zu ersetzen, die aufgrund der Kenntnis aller erforderlichen Daten gewonnen werden".

Weil aber die angestrebte Maximierung der Rationalität an ein Höchstmaß ständig aktualisierter Information gekoppelt wurde, erschien es nur folgerichtig, sich nicht mit den bereits vorhandenen oder herkömmlicherweise verwerteten Daten zufriedenzugeben, sondern die Automatisierung zu nutzen, um immer neue Informationsquellen zu erschließen. Genau darin lag aus der Perspektive all jener, die sich für die integrierte Datenverarbeitung einsetzten, der eigentliche und entscheidende Vorteil des Computers. Er wurde eben keineswegs nur als das denkbar beste Mittel zur Verwaltung existenter Datenbestände betrachtet, vielmehr zuvörderst als das ideale Instrument, um die jeweils vorliegenden Informationen tendenziell unbegrenzt erweitern und ergänzen zu können. Kurzum, indem die automatische Datenverarbeitung sämtliche räumliche Verarbeitungsgrenzen endgültig sprengte, schuf sie zugleich die Voraussetzungen für eine Verarbeitungserwartung, die sich allein an der präsumierten Notwendigkeit der je spezifischen Information für eine im Namen strikter Rationalität und langfristiger Planung agierenden Verwaltung orientierte und deshalb auf die Informationsquelle prinzipiell ebensowenig Rücksicht nahm wie sie sich am Informationsumfang störte.

Je deutlicher sich aber die öffentliche Verwaltung zur Leistungsverwaltung wandelte, desto mehr wuchsen die potentiellen Leistungsempfänger in die Rolle der Informationslieferanten hinein. Weil sie die primären Adressaten der auf sozialen Ausgleich und gesellschaftliche Steuerung bedachten staatlichen Aktivität waren, erschienen sie auch als die natürliche Quelle aller für eine verläßliche Planung sowie für eine korrekte Erfüllung der staatlichen Leistungen benötigten Daten. Die Informationsschuld entwickelte sich, anders ausgedrückt, mehr und mehr zum selbstverständlichen Preis der Leistungsgewährung. In dem Maße daher, in dem die automatisierte Datenverarbeitung Struktur und Tragweite der Informationsverarbeitung in der öffentlichen Verwaltung veränderte, erwies sie sich zugleich als Grundlage einer ständig wachsenden sowie zunehmend verfeinerten Verarbeitung personenbezogener Daten.

Kaum verwunderlich, wenn deshalb Ministerpräsident Osswald in seinen einleitenden Bemerkungen zum „Großen Hessenplan" eher beiläufig, aber doch recht klar feststellte, mit der angestrebten integrierten Datenverarbeitung, ich zitiere: „sind wir in unserem Land auch schon gerüstet für die Einführung eines bundeseinheitlichen Personenkennzeichens als Identifizierungs- und Ordnungsmerkmal in einem neuen Meldegesetz". In der Tat, wer in einer automatisierten und integrierten Verarbeitung ein willkommenes Mittel sieht, um sämtlichen der öffentlichen Verwaltung zur Verfügung stehenden Daten, von wem sie auch immer erhoben sein mögen und wo immer sie sich befinden sollten, alle für die jeweilige Verwaltungsaufgabe erforderlichen Informationen jederzeit zu entnehmen, mußte sich für technische Vorkehrungen aussprechen, mit deren Hilfe sich die einzelnen Daten mühelos miteinander verknüpfen lassen. Just diese Funktion war dem Personenkennzeichen zugedacht. Nichts, aber nichts, schien besser geeignet, eine disparate, weitgehend dem Zufall ausgelieferte und daher der geforderten Rationalität offen zuwiderlaufende Verarbeitung zu beenden, als jeder Bürgerin und jedem Bürger ein den Anforderungen einer ebenso automatisierten wie integrierten Datenverarbeitung voll entsprechendes Identifizierungsmerkmal zuzuteilen, das die Gewähr dafür bieten sollte, entweder die gesamten, eine bestimmte Person betreffenden Daten sofort zusammenzuführen oder aus dem individuellen Datenprofil einzelne, konkret benötigte Angaben genauso schnell herauszufiltern.

Spätestens beim Personenkennzeichen zeigt sich allerdings: Die Landesregierung mag ihre Entscheidung für eine Automatisierung der Verwaltungsabläufe noch so dezidiert formuliert haben. Trotzdem läßt sich von keinem der damit verfolgten Ziele behaupten, es verkörpere bestimmte, lediglich für Hessen typische Positionen und Erwartungen. Im Gegenteil, sowohl die integrierte Datenverarbeitung als auch die Einführung eines einheitlichen Identifizierungsmerkmals gehörten Ende der sechziger, Anfang der siebziger Jahre zu den weit über die Bundesrepublik hinaus vorgebrachten stereotypen Forderungen. Und nicht anders als in Hessen knüpfte sich an ihre Verwirklichung die Hoffnung, dank der Akribie des Computers, die Unanfechtbarkeit der Verwaltungstätigkeit zu gewährleisten sowie die prognostischen Fähigkeiten der Exekutive endgültig jedem Zweifel zu entziehen. Ganz gleich deshalb, ob es um einzelne Bundesländer oder den Bund selbst ging, der Wunsch, möglichst schnell Datenbanken einzurichten und ihre Effektivität nicht zuletzt mit Hilfe eines Personenkennzeichens zu maximieren, beherrschte das Feld. Divergenzen machten sich allenfalls auf der organisatorischen Ebene bemerkbar.

Nur: Hessen ist dabei nicht stehengeblieben. In die Euphorie über die immer wieder angepriesenen, tagtäglich höher eingeschätzten Vorteile der Automatisierung mischte sich von Anfang an ein gehöriges Stück Skepsis. Wer den „Großen Hessenplan" genau liest, stellt alsbald fest: Was zunächst ganz nach einer Ode an den Computer aussieht, schlägt zunehmend in eine kritische Betrachtung der Automatisierungskonsequenzen um. Zweierlei steht dabei im

Vordergrund: die Destabilisierung der Gewaltenteilung und der Verlust jeglicher Privatheit. Eine integrierte Datenverarbeitung verbessert eben nicht nur die Arbeitsbedingungen der Verwaltung, sondern verschafft ihr auch einen Informationsvorsprung und führt damit unweigerlich zu einem Machtzuwachs, der, und ich zitiere jetzt den Hessenplan: „die Effektivität der Mitarbeit der Bürger und der von ihnen gewählten Vertreter in einer demokratischen Ordnung in Frage stellt". Ende des Zitats. Zudem: Die Konzentration der personenbezogenen Daten und ihre Verknüpfung über ein Personenkennzeichen erleichtern zwar in mancherlei Beziehung die Abwicklung staatlicher Leistungen, verändern aber zugleich von Grund auf die Zugriffsbedingungen und ebnen so den Weg für eine tendenziell lückenlose Kontrolle des einzelnen sowie eine gezielte Steuerung seines Verhaltens.

Während jedoch anderswo beides heruntergespielt oder gar verleugnet wurde, fand sich die Hessische Landesregierung nicht dazu bereit. Die mögliche Gefährdung struktureller Prinzipien einer demokratischen Ordnung ließ in ihren Augen nur eine Reaktion zu: So wünschenswert, ja dringend geboten die Automatisierung erschien, so wenig konnte und durfte es angehen, sie zu verwirklichen, ohne zugleich der Exekutive einen Informationszugang zu verwehren, der einem Monopol gleichkam, und außerdem einen uneingeschränkten und unkontrollierten Zugriff auf personenbezogene Daten auszuschließen. Die Prämissen für eine Regelung, die bewußt mit der bis dahin dominierenden Vorstellung brach, dem Gesetzgeber könne, so im Bund, wenn überhaupt nur die Aufgabe obliegen, sämtliche einer reibungslosen Einführung der automatischen Datenverarbeitung entgegenstehenden Hindernisse möglichst schnell aus dem Weg zu räumen, waren damit formuliert. Ziel und Rahmen der legislativen Intervention wurden zum ersten Mal nicht mehr durch rein technokratische Überlegungen, sondern durch verfassungspolitische Reflexionen bestimmt.

Die Konsequenzen blieben jedoch, zunächst jedenfalls, aus. Vergebens sucht man in dem am 16. Dezember 1969 vom Landtag verabschiedeten Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung und Kommunale Gebietsrechenzentren nach Vorschriften, die sich wirklich mit den Gefahren einer automatischen Datenverarbeitung auseinandersetzen. Mehr als eine relativ kurze, eher triviale Feststellung findet sich im Gesetz nicht: § 5 behält das Verfügungsrecht über die Datenbestände demjenigen vor, für den die jeweils in Frage kommenden Daten verarbeitet werden. Niemand wird wohl in Abrede stellen, daß klare Kompetenzzuweisungen mit zu den wichtigsten Bestandteilen einer Regelung zählen, die in Kenntnis der möglichen Verarbeitungsfolgen die Verarbeitungsbedingungen festzulegen sucht. Kaum jemand könnte aber ernsthaft behaupten, derart allgemein gehaltene Zuständigkeitsvorschriften sagten auch nur das Geringste über die notwendigen Reaktionen auf die Konsequenzen einer automatisierten Verarbeitung für die Betroffenen aus. Nicht von ungefähr konzentrierte sich daher die Opposition bei ihrer Kritik vor allem auf diesen Punkt und ebensowenig überrascht es, wenn die Regierung, ganz im Sinn der eigenen Erklärungen, die Notwendigkeit detaillierter Vorkehrungen gar nicht erst abstritt, sondern sich lediglich für eine eigens darauf zugeschnittene gesetzliche Regelung aussprach, die tatsächlich nur wenige Monate später dem Parlament zugeleitet wurde.

So gesehen war der Verlauf der Julidebatte weitgehend vorprogrammiert. Regierung und Opposition hatten sich bereits festgelegt. Beiden erschien ein an den verfassungspolitischen Aspekten der Automatisierung ausgerichtetes Gesetz gleich wichtig. Beide mußten daher ihre Argumentation auf die verfassungspolitischen Gesichtspunkte stützen, in ihnen also den letztlich allein entscheidenden Maßstab für die Beurteilung des Entwurfs erblicken. Der Ministerpräsident wies deshalb jeden Zweifel am Vorrang der Verpflichtung zurück, alles, und ich zitiere: „zu unternehmen, um vermeidbare Gefahren, die die elektronische Datenverarbeitung für Bürger, Regierung und Verwaltung mit sich bringt, von vornherein auszuschließen". Ende des Zitats. Selbst wenn die weitere Entwicklung dazu zwingen sollte, die vorgeschlagenen Bestimmungen zu revidieren, dürfe dies, ich zitiere wieder: „nicht davon abhalten, das jetzt für den Schutz der Bürger und die Sicherung einer demokratischen Regierung Mögliche und Notwendige zu tun". Nicht minder entschieden fiel die Stellungnahme des Abgeordneten Gottfried Milde aus, der für die CDU sprach. Die Vorteile moderner Informationssysteme lägen zwar auf der Hand. Sie rechtfertigten es aber nicht, ich zitiere: „die Unantastbarkeit des Privatlebens, die wesentlichste Errungenschaft von Humanismus und Demokratie in Frage zu stellen". Ende des Zitats. Das zu verhindern sei die Aufgabe des Parlaments und eben deshalb gelte es, das vorgelegte Gesetz als einen „Schritt auf diesem Weg" zu sehen.

Nur, die Reaktion fiel nicht immer so einheitlich aus. Erste Meinungsverschiedenheiten machten sich schon bemerkbar auf einer eher prinzipiellen Ebene, bei der Auseinandersetzung mit den Risiken der Informationstechnologie. Um noch einmal den Abgeordneten Milde zu zitieren: „Der Hinweis auf den Großen Bruder George Orwells", so sagte er, „darf nicht als ironischer Hinweis gesehen werden, sondern wir müssen ihn außerordentlich ernst nehmen. Ein Informationssystem unterliegt nämlich wie jede technische Entwicklung dem Gesetz einer autonomen Entwicklung ... wir müssen sehen, daß ein Riesenspielzeug auch dazu führen kann, daß man unsinnige Spiele damit betreibt. Ich meine, daß diese Einsicht eine wesentliche Voraussetzung dafür ist, daß wir hier diese Rechtsvorschriften behandeln ...". Für den SPD-Abgeordneten Dr. Best Grund genug, von, ich zitiere: „apokalyptischen Visionen" zu sprechen und davor zu warnen, daß es vor allem darauf ankäme, wie er sagte, „die psychologische Schranke zu überwinden, die dem Ausbau der elektronischen Datenverarbeitung und der damit zusammenhängenden Einführung eines zentralen Personenkennzeichens entgegenstünde". Die Antwort des späteren Landtagspräsidenten Dr. Wagner läßt noch einmal deutlich die weitaus vorsichtigere, ja skeptischere Haltung der Opposition gegenüber den sich abzeichnenden technologiebedingten strukturellen Veränderungen der öffentlichen Verwaltung erkennen. „Gerade wir", sagte Dr. Wagner, „als gewählte Vertreter des Volkes sind ja – ich möchte beinahe sagen – direkt beauftragt, von unserer Tätigkeit her, Mißtrauen zu haben – nicht Mißtrauen in destruktivem Sinne, sondern im konstruktiven Sinne, weil wir – und vielleicht in Zukunft mehr denn je – in besonderer Weise die Möglichkeit haben, für den Bürger den Bereich seiner Grundrechte und seiner Freiheitsrechte zu gewährleisten und zu schützen, gerade gegenüber diesen möglichen Einflüssen".

Aber auch bei der Frage, ob die Regierung mit ihren Vorschlägen den eigenen Prämissen wirklich gerecht geworden sei, gingen die Meinungen auseinander. In den Augen der Opposition dokumentierten besonders die Vorschriften zur Stellung und Funktion des Datentenschutzbeauftragten eine höchst widersprüchliche Haltung. Wer in einem unabhängigen Datenschutzbeauftragten die Gewähr für eine wirkliche Kontrolle der Verarbeitung und den Garanten einer kontinuierlichen, gerade im Parlament zu führenden Diskussion über notwendige Verbesserungen des Datenschutzes sehe, der dürfe sich, so meinte die Opposition, weder mit einer Bestellung durch den Ministerpräsidenten abfinden noch mit der Verpflichtung, der Regierung zu berichten. Der Datenschutzbeauftragte müsse vielmehr durch das Parlament gewählt werden und diesem gegenüber zur Rechenschaft verpflichtet sein.

Die Kritik blieb nicht ohne Folgen. Die Ausschußberatungen führten vor allem dazu, die Wahl des Datenschutzbeauftragten durch den Landtag vorzusehen, dem Parlament, seinem Präsidenten, den Fraktionen sowie den kommunalen Vertretungsorganen das Recht einzuräumen, vom Datenschutzbeauftragten zu verlangen, der Frage nachzugehen, weshalb die Regierung oder die jeweils zuständige kommunale Stelle ein bestimmtes Auskunftsersuchen nicht beantwortet habe und schließlich der Regierung die Möglichkeit zu nehmen, sich schlicht auf das „öffentliche Interesse" zu berufen, um dem Parlament den Zugang zu den automatisiert verarbeiteten Daten zu verwehren. Am 30. September 1970 wurde dann mit den Stimmen der SPD, der CDU und der F.D.P., bei Stimmenthaltung der NPD das erste Datenschutzgesetz der Welt angenommen. Im Mai 1973 folgte Schweden dem hessischen Beispiel, im November 1976 verabschiedete der Bundestag das Bundesdatenschutzgesetz und im Januar 1978 die französische Nationalversammlung das Gesetz über die Datenverarbeitung, die Dateien und die Freiheitsrechte.

Spätestens aber seit der Datenschutzkonvention des Europarates vom 28. Januar 1981 kann es keinen Zweifel mehr geben: Der Hessische Landtag hat mit seiner zuweilen als Musterbeispiel provinzieller Exotik belächelten Entscheidung die Grundlage für eine der national wie international wichtigsten legislativen Entwicklungen der letzten Jahrzehnte geschaffen. Der wohl jüngste Beweis dafür sind die Mitte Juli dieses Jahres vorgelegten Vorschläge für eine Datenschutzrichtlinie der Europäischen Gemeinschaft. Sie knüpfen genau dort an, wo auch der Hessische Landtag vor nunmehr zwanzig Jahren angesetzt hatte, bei der konstitutiven Bedeutung zwingender Anforderungen an die Verarbeitung personenbezogener Daten für die Grundrechte des einzelnen und damit für die Existenz und Funktionsfähigkeit einer demokratischen Gesellschaft.

Der Erfolg des Hessischen Datenschutzgesetzes demonstriert aber auch, und zwar nicht minder eindrucksvoll, Notwendigkeit und Chancen einer konsequent wahrgenommenen Regelungskompetenz des Landesgesetzgebers. Weder bei den Vorarbeiten zum Entwurf noch bei der parlamentarischen Beratung hat, nicht einmal andeutungsweise, die Überlegung eine Rolle gespielt, erst die Reaktion des Bundes abzuwarten. Im Gegenteil, Parlament und Regierung waren sich durchweg ihrer Vorreiterfunktion bewußt. Sie wollten geradezu den Kompetenzspielraum des Landes voll nutzen, um damit einen in die gleiche Richtung zielenden Gesetzgebungsprozeß bei den anderen Ländern ebenso wie beim Bund auszulösen. Die Entwicklung hat ihnen recht gegeben. Mehr noch, ohne die zunächst von einem weiteren Land, Rheinland-Pfalz, aufgegriffene Initiative Hessens und die späteren immer wieder von der Landesgesetzgebung ausgehenden Impulse hätte der Datenschutz niemals seinen gegenwärtigen Stand erreicht.

Anders und pointierter formuliert: Der Bundesgesetzgeber ist sowohl 1976 als auch bei der gerade abgeschlossenen Novellierung des Bundesdatenschutzgesetzes hinter den im Landesbereich akzeptierten Anforderungen zurückgeblieben. So definierte der Bundesgesetzgeber 1976 den Datenschutz, im Unterschied zu den hessischen Bestimmungen, als eine Regelung, deren Aufgabe es sein müsse, den Mißbrauch bei der Verarbeitung personenbezogener Daten zu verhindern und leistete damit über Jahre allen auf eine möglichst restriktive Anwendung des Datenschutzes bedachten Bestrebungen Vorschub. 1990 gelang es zwar in letzter Minute, die Erhebung personenbezogener Daten ebenso wie deren Verarbeitung in Akten zumindest für den öffentlichen Bereich in die Novelle einzubeziehen. Sämtliche Versuche, die hartnäckig verteidigten Einschränkungen der Kontrollkompetenz des Bundesbeauftragten für den Datenschutz ersatzlos zu streichen und damit die vorgesehene Regelung den in einer ganzen Reihe von Landesgesetzen mittlerweile enthaltenen Vorschriften anzupassen, scheiterten hingegen.

Zugegeben, der Landesgesetzgeber ist bei der Verabschiedung des 2. Hessischen Datenschutzgesetzes, Ende 1978, den eigenen, 1970 formulierten Ansprüchen nur partiell gerecht geworden. Der Grund ist lehrreich genug. An Vorschlägen, die unmittelbar an die Tradition des Gesetzes von 1970 knüpften und deshalb durchaus darauf bedacht waren, die Eigenständigkeit der hessischen Regelung zu demonstrieren, ohne im übrigen die Entwicklung im Bundesbereich außer acht zu lassen, mangelte es keineswegs. Sie wurden aber unter Hinweis auf ihre Unvereinbarkeit mit dem Regelungsmodell des Bundes größtenteils gar nicht erst richtig diskutiert. Dennoch gelang es, vor allem im Laufe der parlamentarischen Beratungen, den Regierungsentwurf um eine Reihe von Vorschriften zu ergänzen, die etwa den Betroffenen einen Schadenersatzanspruch bei einer rechtswidrigen Verwertung ihrer Daten gewährten oder die Zweckbindung bei der Verarbeitung verschärften und damit den vom Bundesgesetzgeber eingeschlagenen Weg verließen. Zwölf Jahre später fällt es nicht schwer, festzustellen, daß gerade diese Bestimmungen den Anstoß für wichtige, in die Novellierung aufgenommene Korrekturen des Bundesdatenschutzgesetzes gegeben haben.

Wie sehr sich aber der Landtag nach wie vor der Pionierrolle Hessens bewußt war, zeigte sich besonders deutlich bei der Debatte über die Stellung des Datenschutzbeauftragten. Die Landesregierung hatte einmal mehr gemeint, sich an die Vorlage des Bundes halten zu müssen und deshalb den Datenschutzbeauftragten organisatorisch dem Innenminister zugeordnet. Die Abgeordneten aller Fraktionen erinnerten die Landesregierung an die Entscheidung des Hessischen Gesetzgebers für eine Anbindung des Datenschutzbeauftragten an das Parlament, lehnten die

Regierungsvorschläge einmütig ab und sprachen sich ebenso einhellig für eine Regelung aus, die nicht nur den Grundgedanken des Gesetzes von 1970 entsprach, sondern diese auch konsequent weiterführte: eine nunmehr auch organisatorische Verknüpfung mit dem Parlament.

Erst mit dem im November 1986 verabschiedeten 3. Datenschutzgesetz übernahm der Landesgesetzgeber wieder voll seine Pionierfunktion. Ende 1983 hatte das Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz nicht nur die in der Verfassung begründete Verpflichtung des Gesetzgebers bekräftigt, verbindliche Vorkehrungen für die Verarbeitung personenbezogener Daten zu treffen, sondern auch eine Reihe präzise umschriebener Erwartungen an seine Adresse formuliert. Ähnlich wie 1970 galt es deshalb zu fragen, wie den Konsequenzen einer quantitativ ständig zunehmenden und qualitativ immer weiter verfeinerten Verarbeitung am besten begegnet werden könnte, diesmal allerdings vor dem Hintergrund der Erfahrungen mit den bestehenden Gesetzen und der Vorgaben des Bundesverfassungsgerichts. Und genau wie damals hat der Hessische Gesetzgeber nicht auf den Bund gewartet, sondern wiederum als erster reagiert.

Ganz gleich zudem, ob man die frühesten Vorarbeiten, die im Laufe der parlamentarischen Beratungen entwickelten Vorschläge oder die endgültige Fassung nimmt, ausschlaggebend war stets die Überzeugung, daß es einzig und allein darauf ankommen müsse, eine strikt an den Zielen des Datenschutzes und nicht an irgendwelchen anderen Vorschriften ausgerichtete Regelung zu finden. Nur deshalb war es möglich, sich von der historisch erklärlichen, sachlich jedoch völlig ungerechtfertigten Anknüpfung der Datenschutzvorschriften an die Verarbeitung in Dateien zu lösen und sich statt dessen lediglich dafür zu interessieren, ob personenbezogene Angaben genutzt würden; die Erhebung genauso in den Anwendungsbereich der gesetzlichen Vorschriften einzubeziehen wie jede andere Verarbeitungsphase; eine bessere Information der Betroffenen mit Hilfe einer Benachrichtigungspflicht anzustreben sowie schließlich jene gesetzlich verankerten Einschränkungen der Kontrollbefugnisse des Datenschutzbeauftragten zu beseitigen, die nicht nur die Wirksamkeit der Überwachung gefährdeten, sondern auch die Glaubwürdigkeit seiner Tätigkeit in Frage stellten. Jede dieser Entscheidungen war zugleich Baustein einer Regelung, die genauso wie 1970 weit über die Grenzen des Landes hinaus alle Versuche, den Datenschutz neu und besser zu gestalten beeinflußt und zu guter Letzt auch den Bundesgesetzgeber veranlaßt hat, seine Vorschläge wenigstens teilweise zu revidieren.

Kurzum, die Geschichte aller drei hessischen Datenschutzgesetze beweist: Der Preis für die Bereitschaft, zentralistischen Bestrebungen nachzugeben, die im Namen einer falsch verstandenen Einheitlichkeit propagiert wurden, sind stets Regelungen gewesen, die letztlich mehr zur Konservierung eingefahrener Verarbeitungspraktiken als zum Schutz der Betroffenen beigetragen haben. Der Datenschutz hat deshalb nur solange eine Chance, wirklich ernst genommen und konsequent gewährleistet zu werden, wie die Landesgesetzgeber dezidiert auf ihrer Kompetenz beharren und sie zugleich als Anreiz verstehen, sich jedem Rückschritt zu widersetzen sowie für eine kontinuierliche Weiterentwicklung zu sorgen.

Wie sehr es darauf ankommt, zeigen die ersten Erfahrungen mit der Novellierung des Bundesdatenschutzgesetzes. Sie lehnt, im Gegensatz zu den hessischen Regeln, nicht nur nach wie vor eine uneingeschränkte Kontrollbefugnis des Bundesbeauftragten ab, sondern bestimmt zugleich, daß die vorgesehenen Schranken von den jeweils zuständigen Kontrollinstanzen der Länder zu beachten sind. Streiten läßt sich nun allenfalls darüber, ob es dem Bundesgesetzgeber ohne weiteres gestattet sein kann, die Datenschutzbeauftragten der Länder zu verpflichten, sich bei der Überprüfung der Anwendung von Bundesgesetzen in einer Weise zu verhalten, die ihren gesetzlich garantierten Befugnissen offen zuwiderläuft. Hingegen dürfte es keinen Zweifel geben, daß es dem Bundesgesetzgeber untersagt ist, in Regelungsbereiche einzugreifen, die ausschließlich der Kompetenz des Landesgesetzgebers unterliegen. Trotzdem zeichnen sich immer deutlicher Bestrebungen ab, sich auf Einschränkungen, die für den Bundesbeauftragten gelten, etwa bei Kontrollen von Personalakten oder der im Rahmen einer Sicherheitsüberprüfung zusammengestellten Unterlagen selbst dann zu berufen, wenn die Angaben eindeutig von einer Landesbehörde im Hinblick auf eine ihr durch ein Landesgesetz zugewiesene Aufgabe erhoben worden sind.

Gewiß, jedes der drei hessischen Datenschutzgesetze hat seine Geschichte. Und doch haben von Anfang an drei Grundsätze die parlamentarischen Beratungen ebenso beherrscht wie die legislativen Entscheidungen geprägt.

Der Hessische Gesetzgeber hat, erstens, die Frage nach einer Regelung der Datenverarbeitung stets unter dem Gesichtspunkt der Anforderungen beurteilt, die in einer demokratischen Gesellschaft an die Verteilung von Information gestellt werden müssen, ohne Rücksicht im übrigen darauf, ob die jeweils betroffenen Daten personenbezogen sind oder nicht. Die Chancen der parlamentarischen Gremien sowie die Möglichkeiten des einzelnen, sich an den politischen und gesellschaftlichen Entscheidungsprozessen zu beteiligen, bestimmen sich in der Tat auch und gerade danach, unter welchen Voraussetzungen Informationen erhoben, verarbeitet und verbreitet werden. Wo die Verarbeitung arkanisiert und von Informationsprivilegien begleitet wird, die nicht in einem demokratisch gestalteten, öffentlichen Verfahren begründet, diskutiert und akzeptiert worden sind, ist eine wachsende Manipulierbarkeit die unweigerliche Folge. Solange es deshalb, zumal unter den Bedingungen einer Technologie, die den jederzeitigen Zugriff für jeden nur gewünschten Zweck erlaubt, an verbindlichen Verarbeitungsregeln fehlt, sind Parlament und Bürger gleichermaßen in ihrer Handlungsfähigkeit gefährdet.

Aus genau diesem Grund hat sich der Hessische Gesetzgeber bereits 1970 für eine zweispurige Regelung entschieden und auch später an ihr festgehalten. Keines der drei Gesetze fügt sich daher in das übliche Regelungsschema, das den Datenschutz ausschließlich unter dem Gesichtspunkt der Verarbeitung personenbezogener Daten behandelt. Der Verlust jeglicher Kontroll- und Initiativmöglichkeit des Parlaments durch einen systematisch ausgebauten, technisch

abgesicherten Informationsvorsprung der Regierung und die Degradierung der Bürgerinnen und Bürger zu einem, dank der minutiösen Verarbeitung einer Vielzahl von Daten zu ihrer Person, beliebig steuerbarem Objekt staatlicher Politik sind für den Hessischen Gesetzgeber Teil ein und derselben, die Existenz einer demokratischen Gesellschaft unmittelbar berührenden Frage und müssen infolgedessen auch Bestandteile einer Regelung sein.

Eine so konzipierte Regelung enthält notwendigerweise ein drittes, in allen drei Gesetzen allerdings nur punktuell angesprochenes Element: die Aktenöffentlichkeit. Genaugenommen taucht sie an zwei ganz verschiedenen Stellen auf, bei den Informationsrechten des Parlaments und den für die wissenschaftliche Forschung geltenden Verarbeitungsbedingungen. In beiden Fällen kommt aber deutlich die später durch das Archivgesetz erneut und eindringlich bekräftigte Überzeugung zum Ausdruck, daß es ohne ein Höchstmaß an Transparenz der öffentlichen Verwaltung keine wirklich von den parlamentarischen Gremien ebenso wie von den Bürgerinnen und Bürgern gestalteten politischen und sozialen Entscheidungsprozesse geben kann. Kurzum, die Trias von Informationsgleichgewicht, Schutz der personenbezogenen Daten und Aktenöffentlichkeit bestimmt Entstehung und Eigenart des hessischen Regelungskonzepts. Keines dieser Elemente läßt sich deshalb herauslösen oder gegen die übrigen ausspielen, ohne das seit 1970 immer wieder bestätigte Ziel des Gesetzgebers in Frage zu stellen, ein Informationssystem zu schaffen, das den Funktionsbedingungen einer demokratischen Gesellschaft genügt.

Weil aber auch und vor allem die Handlungsfähigkeit des einzelnen von Anfang an Leitmaßstab der legislativen Intervention war, hat sich der Gesetzgeber, zweitens, bei der Forderung, den möglichen Konsequenzen der Verwendung personenbezogener Daten vorzubeugen, ausschließlich an der Verarbeitung selbst orientiert, sich also weder auf qualitative Unterscheidungen zwischen den einzelnen Angaben eingelassen noch seinen Eingriff von einem bestimmten Verhalten der jeweils speichernden Stelle abhängig gemacht. Nicht von ungefähr sprach deshalb der erste Hessische Datenschutzbeauftragte, Willi Birkelbach, von einer „Datenverkehrs-Ordnung". Wer immer, mit anderen Worten, sich für personenbezogene Daten interessiert, kann und darf nur unter bestimmten im voraus präzise definierten Bedingungen auf sie zugreifen. Genau diese Feststellung sollte dreizehn Jahre später, im Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz wiederkehren. Und nicht anders als zuvor der Hessische Gesetzgeber sieht das Gericht in einer so verstandenen Regelung den entscheidenden normativen Ansatz, um den einzelnen davor zu bewahren, für alle möglichen, an ihm vorbei festgelegten Zwecke instrumentalisiert zu werden. Konsequenterweise steht deshalb auch für das Bundesverfassungsgericht fest: In dem Maße, in dem auf verbindliche, jede Nutzung personenbezogener Daten einbeziehende sowie gerade für die Betroffenen erkennbare und nachvollziehbare Verarbeitungsanforderungen verzichtet wird, steigen die Chancen, auf das Verhalten der Betroffenen Einfluß zu nehmen und schwindet ihre Kommunikations- und Handlungsfähigkeit.

Sichtbar wird daran auch so viel: Weder der Hessische Gesetzgeber noch das Bundesverfassungsgericht haben mit ihren Forderungen einen wie immer verstandenen „Rückzug in die Privatheit" eingeläutet oder sich gar für eine „Atomisierung" der Gesellschaft ausgesprochen. Für beide ist vielmehr eine gesetzlich abgesicherte informationelle Selbstbestimmung nicht etwa ein Mittel, um sich der Gesellschaft zu verschließen, sondern im Gegenteil die Grundvoraussetzung dafür, sie für sich erschließen zu können.

Der Hessische Gesetzgeber hat deshalb in einer Gesellschaft, in der es mittlerweile zur Selbstverständlichkeit geworden ist, immer neue Informationserwartungen an die Adresse der Bürgerinnen und Bürger zu formulieren sowie zugleich mit Hilfe einer systematischen Verarbeitung ihrer Daten Entscheidungen zu fällen, die sich unmittelbar auf ihre persönlichen Existenzbedingungen und Entwicklungschancen auswirken, mit den von ihm sanktionierten Verarbeitungsanforderungen weit mehr getan, als nur den habeas corpus act durch einen habeas data act ergänzt. Das Datenschutzgesetz schlägt die Brücke zur „civil society", einer Gesellschaft also, die sich zuvörderst auf die Mitwirkung ihrer Bürgerinnen und Bürger gründet und daher in deren Bereitschaft und Fähigkeit, sich nicht zuletzt mit Hilfe der ihnen garantierten Rechte an der Gestaltung der politischen und sozialen Prozesse zu beteiligen, die letztlich einzig mögliche Legitimation sozialer und politischer Organisation sieht.

Der Hessische Gesetzgeber hat, drittens, von Anfang an keinen Zweifel gelassen, daß alle Bemühungen, bestimmte Verarbeitungsvorkehrungen festzulegen, reine Sandkastenspiele bleiben müssen, wenn nicht zugleich eine unabhängige Instanz mit dem doppelten Ziel eingerichtet wird, die Anwendung der Datenschutzbestimmungen zu kontrollieren sowie die weitere Entwicklung der Verarbeitung zu analysieren. Hans-Joachim Reh, der als langjähriger Mitarbeiter zunächst der Staatskanzlei, später des Hessischen Datenschutzbeauftragten wie kaum ein anderer Entstehung und Fortgang der gesetzlichen Regelung verfolgt und mitgestaltet hat, beschreibt die Gründe dafür so: „Es genügt nicht, darauf zu vertrauen, daß der betroffene Bürger die ihm in der Datenschutzgesetzgebung eingeräumten Rechte zur Wahrung seines Freiheitsraumes ausüben wird. Die vielfältigen Abhängigkeiten des Individuums ... erschweren oder verhindern eine rigorose Durchsetzung individueller Ansprüche. Die hergebrachten rechtsstaatlichen Sicherungen, wie die Rechtsweggarantie und das Petitionsrecht, sind unzulänglich; .... vor allem deswegen, weil sie Schäden oder Nachteile des Bürgers nicht vorbeugend verhindern, sondern vornehmlich darauf gerichtet sind, eingetretene Schäden oder Nachteile wieder gut zu machen."

Auf den ersten Blick mag es daher seltsam, ja widersprüchlich erscheinen, sich einerseits für einen konsequenten Datenschutz gerade um der Handlungs- und Mitwirkungsfähigkeit der Bürgerinnen und Bürger willen einzusetzen, andererseits jedoch die Verarbeitungskontrolle nicht als eine ausschließlich den Betroffenen vorbehaltene, sondern vornehmlich einer eigens dafür eingerichteten Instanz obliegende Aufgabe anzusehen. In Wirklichkeit hat der Gesetzgeber keine Alternative. Allein schon die Komplexität der Verwaltungsabläufe, aber auch der Verarbeitungsprozesse zeigt die Grenzen einer Intervention der Betroffenen auf. Jede, noch so intensiv durchgeführte

individuelle Kontrolle bleibt zudem zwangsläufig auf den Einzelfall beschränkt. Wenn jedoch die gesetzliche Regelung tatsächlich dazu verhelfen soll, strukturelle Änderungen der Verarbeitung ebenso durchzusetzen wie auf die möglichen Auswirkungen der Informationstechnologie rechtzeitig zu reagieren, dann genügen punktuelle, individuell motivierte Kontrollen nicht. Nur eine systematische, breit angelegte, sich mit den Hintergründen und den Konsequenzen der Verarbeitungserwartungen der je spezifischen Behörde genauso wie mit den inneradministrativen Interdependenzen auseinandersetzende Überwachung kann diesem Ziel zumindest nahekommen.

Wer deshalb dafür plädiert, die institutionelle Kontrolle zugunsten einer individuellen Überwachung zurückzudrängen, womöglich gar ganz abzuschaffen, erliegt entweder einer Illusion oder, schlimmer noch, preist die Rechte der Betroffenen an, um die Intervention des Datenschutzbeauftragten, soweit es nur irgendwie geht, auszuschalten. Die lange Debatte über das mittlerweile vom Bundesgesetzgeber, wenn auch in abgeschwächter Form akzeptierte Recht des Betroffenen, einer Kontrolle durch den Bundesbeauftragten zu widersprechen, ist das jüngste Beispiel dafür.

Eben deshalb hat sich der Hessische Gesetzgeber bei allem Respekt vor den Rechten der Betroffenen für einen Datenschutzbeauftragten entschieden und damit, in den Worten Willi Birkelbachs, eine „Gegenmacht" institutionalisiert. Entstanden ist auf diese Weise eine Instanz, die zwar in mancherlei Hinsicht den Einfluß der Vorstellungen über die „Bürgerbeauftragten" erkennen läßt, deren Aufgaben und Kompetenzen aber ohne Vorbild sind. Die Garantien ihrer Unabhängigkeit und der Umfang ihrer Rechte bestimmen letztlich die Transparenz der Verarbeitungsprozesse ebenso wie die Chancen, der vor allem einer Verwertung personenbezogener Daten stets anhaftenden Gefahr rechtzeitig entgegenzuwirken, demokratische Strukturen unmerklich aber um so wirksamer zu unterlaufen.

Der Blick zurück schärft das Bewußtsein für Entwicklungen, die zwar in der Entscheidung des Hessischen Gesetzgebers für eine Verarbeitungsregelung angelegt sind, ihr aber, so merkwürdig es klingen mag, eindeutig widersprechen:

Der Gesetzgeber mußte sich beispielsweise aus Kompetenzgründen mit Vorschriften zufriedengeben, die sich an die Landesverwaltung richten. Ganz gleich deshalb, ob es um die ersten tastenden Versuche geht, den Datenschutz sicherzustellen oder die späteren Initiativen, ihn weiter auszubauen, formuliert wurden stets Anforderungen an die Adresse des öffentlichen Bereichs. Je schärfer aber die Verarbeitungsbedingungen ausfielen und je konsequenter sie gehandhabt wurden, desto deutlicher zeichnete sich die Diskrepanz zum privaten Bereich ab. Mehr und mehr gerät unter diesen Umständen der Datenschutz zu einem in Hessen ebenso wie überall sonst in der Bundesrepublik auf die staatliche Tätigkeit beschränkten Regelungskomplex.

Gewiß, Bestimmungen, die sich auf den privaten Bereich beziehen, bestehen durchaus. Nur werden just jene Regelungselemente ausgespart, ohne die es einen wirklich wirksamen Datenschutz gar nicht erst geben kann, angefangen bei der strikten Zweckbindung über die Einbeziehung aller Verarbeitungsformen bis hin zu einer öffentlichen Diskussion der Verarbeitungspraktiken und einer Kontrolle nach genau den Grundsätzen, die auch für den öffentlichen Bereich gelten. Der Hessische Gesetzgeber hat zwar hier ebenfalls versucht, im Rahmen seiner Möglichkeiten zu reagieren, wie sich etwa an der in das 3. Hessische Datenschutzgesetz aufgenommenen Berichtspflicht der für den privaten Bereich zuständigen Aufsichtsbehörden zeigt. Nicht einmal die, dank dieser Vorschrift, inzwischen öffentlich dokumentierten negativen Erfahrungen konnten jedoch den Bundesgesetzgeber dazu bewegen, die längst fälligen Korrekturen vorzunehmen.

Weder der Hessische Gesetzgeber noch das Bundesverfassungsgericht haben freilich Grundsätze formuliert, die lediglich vor dem Hintergrund der staatlichen Tätigkeit verständlich und deshalb nur auf sie anzuwenden sind. Beide haben im Gegenteil eine Entwicklung angesprochen, die national wie international niemals an den Grenzen des öffentlichen oder des privaten Bereiches halt gemacht und daher durchweg die Gefahren ausgelöst hat, denen sowohl der Hessische Gesetzgeber als auch das Bundesverfassungsgericht begegnen wollten. Solange jedoch der Widerspruch zwischen den für die beiden Bereiche geltenden Verarbeitungsanforderungen nicht behoben, ja noch weiter vertieft wird, klammert die Datenschutzgesetzgebung faktisch entscheidende Teile der Lebenswelt des einzelnen aus und stellt damit ihre in der Verfassung begründete Prämisse in Frage, seine Handlungs- und Kommunikationsfähigkeit zu sichern.

Der Hessische Gesetzgeber hat ferner mit der Verabschiedung des 1. Datenschutzgesetzes eine Verrechtlichung, genauer noch eine Vergesetzlichung der Verarbeitungsanforderungen eingeleitet. Ganz in diesem Sinn hat das Bundesverfassungsgericht jeden Zweifel daran beseitigt, daß alle Einschränkungen der informationellen Selbstbestimmung einer gesetzlichen Grundlage bedürfen. Die wohl deutlichste Konsequenz dieser Feststellung ist die fortschreitende Verdrängung der allgemeinen Datenschutzvorschriften durch bereichsspezifische Bestimmungen. Die Vergesetzlichung konkretisiert freilich sowohl aus der Perspektive des Hessischen Gesetzgebers als auch aus der Sicht des Bundesverfassungsgerichts eine materiale Forderung. Die Verpflichtung, den Gesetzgeber einzuschalten, zwingt nicht nur dazu, die jeweiligen Verarbeitungserwartungen offenzulegen. Sie hat vielmehr genauso zur Folge, daß der Zugriff auf personenbezogene Daten keine Selbstverständlichkeit ist, sondern vor dem Hintergrund eines exakt umschriebenen Verarbeitungszusammenhangs legitimiert und vom Parlament gebilligt werden muß.

Zunehmend machen sich jedoch Tendenzen bemerkbar, die ursprünglich material verstandene Forderung nach einer Vergesetzlichung der Verarbeitungsbedingungen in ein rein formales Erfordernis umzudeuten. Statt also die

Notwendigkeit einer legislativen Entscheidung zunächst und vor allem zum Anlaß zu nehmen, um die eigenen Verarbeitungspraktiken kritisch zu überprüfen und zugleich die jeweiligen Verarbeitungserwartungen soweit wie möglich einzuschränken, wird die Intervention des Gesetzgebers lediglich als formaler Akt gesehen, mit dessen Hilfe daher sowohl die bisherigen Verarbeitungsvorgänge als auch neue Verarbeitungswünsche mehr oder weniger problemlos abgedeckt werden können. Noch einmal aber: Der Hessische Gesetzgeber hat sich weder 1970 noch und erst recht sechzehn Jahre später, als es keinen Zweifel an der zentralen Bedeutung bereichsspezifischer Vorschriften mehr geben konnte, eher zufällig für die Vergesetzlichung ausgesprochen. Die Hinwendung zum Gesetz erschien ihm vielmehr als der einzig richtige Weg, um eine an den Grundprinzipien des Datenschutzes wirklich orientierte Verarbeitungsregelung sicherzustellen. Jeder Versuch, die Interventionspflicht des Gesetzgebers zu entmaterialisieren kommt deshalb einem Bruch mit jenen Prinzipien gleich, die 1970 den Eingriff des Gesetzgebers ausgelöst haben und danach immer wieder bestätigt wurden.

Die Geschichte der Datenschutzregelungen läßt schließlich erkennen, welch großen Wert der Hessische Gesetzgeber normativen Vorgaben beigemessen hat. Er distanzierte sich damit ausdrücklich von jener, Anfang der siebziger Jahre weit verbreiteten Sicht, die Datenschutz schlicht mit Datensicherheit gleichsetzte. So berechtigt jedoch diese Einstellung ist, so leicht verführt sie dazu, die Bedeutung zu unterschätzen, die der Informationstechnologie gerade unter Datenschutzaspekten zukommt. Der Gesetzgeber hat nur solange eine Chance, die Verarbeitungsgefahren aufzufangen, wie es ihm gelingt, den Wettlauf mit einer sich rapide verändernden Verarbeitungstechnologie einigermaßen zu bestehen. Deshalb gilt es, von der Vorstellung einer linearen, längst bekannte Verarbeitungsformen einfach potenzierenden Entwicklung der Informationstechnologie ebenso Abschied zu nehmen, wie von der Meinung, nicht mehr tun zu müssen, als die einmal geschaffene gesetzliche Grundlage lediglich punktuell zu korrigieren.

Mit der wachsenden Verbreitung der Personal Computer und der Einführung von ISDN, um nur diese beiden Beispiele zu nehmen, änderten sich nicht nur die Verarbeitungsbedingungen von Grund auf, sondern auch die Voraussetzungen einer rechtlichen Regelung. Konkret: Wo eine dezentrale Verarbeitung vorherrscht, versagen zwangsläufig alle Vorkehrungen, die unter dem Eindruck einer scheinbar unumkehrbaren Zentralisierung entwickelt worden sind, von den Übermittlungsanforderungen bis hin zur Kontrollstruktur. Zugleich wird aber deutlich: Keiner der traditionellen rechtlichen Ansatzpunkte führt weiter. Abhilfe kann nur eine gezielte Integration der Datenschutzanforderungen in die Produktion der Soft- und Hardware bieten.

Normative Vorgaben, wie etwa die Einschränkung der Verarbeitungsmöglichkeiten durch präzise Aussagen zu den Aufgaben der einzelnen verarbeitenden Stellen und eine klare Zweckbindung oder die Absicherung der informationellen Selbstbestimmung über eine rechtlich garantierte Beteiligung am Verarbeitungsprozeß, sind zwar nach wie vor unerläßlich. Die Zukunft des Datenschutzes hängt aber mehr denn je von der Entwicklung einer eigens am Datenschutz ausgerichteten Technologie ab.

Kurzum, zwanzig Jahre nach der Verabschiedung des ersten Hessischen Datenschutzgesetzes bestätigt sich zum wiederholten Mal jener in der Julidebatte des Jahres 1970 vom Ministerpräsidenten Albert Osswald ebenso wie vom CDU-Abgeordneten Milde formulierte Vorbehalt: Die Datenschutzgesetze können nicht mehr als eine vorläufige Reaktion auf die politischen und sozialen Konsequenzen der Informationstechnologie sein. Jedes dieser Gesetze trägt zwar dazu bei, die Erfahrungen im Umgang mit der Verarbeitung zu vergrößern und ist insofern ein wichtiger Anreiz für weitere Reflexionen über Voraussetzungen und Grenzen des Datenschutzes, bleibt aber stets nur eine Zwischenetappe eines offenen Regelungsprozesses.

17.2
Berichte des Hessischen Datenschutzbeauftragten und Bericht der Landesregierung zu den Äußerungen des Innenministers Milde im Plenum des Hessischen Landtags am 24. Oktober 1990

17.2.1
Bericht des Hessischen Datenschutzbeauftragten vom 9. Oktober 1990 auf Beschluß des Hauptausschusses vom 25. Oktober 1990

(zur Veröffentlichung bestimmte Fassung des Berichts vom 8. November 1990)

1. Auftrag und Gegenstand des Berichts

In der Sitzung des Hauptausschusses vom 25. Oktober 1990 bin ich gebeten worden, „den vom Minister des Innern in der Plenardebatte vorgetragenen Sachverhalt unter datenschutzrechtlichen Gesichtspunkten zu prüfen und dem Ausschuß bis zu seiner nächsten Sitzung über das Ergebnis dieser Prüfung schriftlich zu berichten" (Beschlußprotokoll der 43. Sitzung des HAA, zu Punkt 7). Diesen Wunsch des Ausschusses sehe ich als Auftrag nach § 25 HDSG an. Danach kann der Landtag den Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen. Unberührt bleibt meine autonome Überwachungsbefugnis für die Einhaltung des HDSG und anderer Vorschriften über den Datenschutz bei allen hessischen Behörden nach § 24 Abs. 1 HDSG.

Der Untersuchungsrahmen ebenso wie die in diesem Bericht zu ziehenden Schlußfolgerungen waren und sind in mehrerlei Hinsicht eingegrenzt:

1. Wegen der Kürze der mir für diesen Bericht zur Verfügung stehenden Zeit ist es ausgeschlossen, alle möglicherweise datenschutzrechtlich relevanten Details zu ermitteln, darzustellen und rechtlich zu bewerten. Ich beschränke mich daher strikt auf die Aufbewahrung und Weitergabe des fraglichen „Abhörprotokolls" vom 30. Januar 1990 bzw. der aus ihm gefertigten Vermerke und Zusammenfassungen sowie die Verwendung von Informationen aus diesen Dokumenten im Redebeitrag von Staatsminister Milde im Plenum am 24. Oktober 1990.

2. Wegen der umfassenden Ermittlungen zu diesem ursprünglichen Auftrag des Ausschusses war es nicht möglich, nachträglich die Untersuchung in dem von der SPD-Fraktion (Schreiben vom 30. Oktober 1990) gewünschten Umfang zu erweitern. Der Vorsitzende des Hauptausschusses hatte mir in seinem Schreiben vom 31. Oktober 1990 anheimgestellt, so zu verfahren. Schon aus Zeitgründen war es ausgeschlossen, die Fragen einzubeziehen, ob und inwieweit Unterlagen oder Mitteilungen über den Inhalt des fraglichen Telefonats u.a. auch an die Pressestellen von Innenministerium und CDU-Landtagsfraktion weitergegeben worden sind. Hinzu kommt, daß darüber hinaus weitere Adressaten in Regierung, Parlament und Medien in Betracht kommen, die dann ebenfalls einzubeziehen wären.

3. Mir stehen staatsanwaltschaftliche Befugnisse bei der strafrechtlichen Würdigung des Sachverhalts nicht zu. Zur Strafbarkeit einzelner Beteiligter, die bekanntlich auch eine Wertung der subjektiven Tatbestandsmerkmale einschließt, treffe ich daher keinerlei Aussage.

4. Für die Untersuchung von Vorgängen im Bundeskriminalamt habe ich keine Zuständigkeit. Was die Verwendung und Weitergabe der fraglichen Unterlagen im und aus dem BKA angeht, muß ich mich beziehen zum einen auf die Aussagen der beteiligten hessischen Beamten, zum anderen auf Feststellungen des von mir eingeschalteten Bundesbeauftragten für den Datenschutz.

5. Die in diesem Bericht dargestellten Vorgänge und Abläufe zeigen strukturelle Probleme des Umgangs mit personenbezogenen Daten in einzelnen beteiligten Stellen auf, die in Abschnitt 4 nur stichwortartig benannt werden können. Ich habe vor, diese aus meiner Sicht erforderlichen Konsequenzen in den nächsten Monaten mit dem Innen- und dem Justizministerium zu erörtern.

Zur Aufklärung des Sachverhalts wurden persönliche und telefonische Gespräche u.a. mit Minister Milde, Staatssekretär Bouffier, dem Leiter der Staatsanwaltschaft in Frankfurt/M., leitenden Beamten der Polizeiabteilung des Innenministeriums sowie den in dem Gesamtkomplex Beker u.a. ermittelnden Staatsanwälten geführt.

Bei meiner Überprüfung sind mir von sämtlichen beteiligten hessischen Stellen alle erforderlichen Dokumente zur Verfügung gestellt und alle gewünschten Auskünfte erteilt worden.

2. Sachverhalt

Meine Ermittlungen haben zu folgendem Ergebnis geführt:

Auf Antrag der Staatsanwaltschaft beim Landgericht Frankfurt/M. ordnete das Amtsgericht Frankfurt/M. durch Beschluß vom 24. November 1989 im Rahmen eines Ermittlungsverfahrens die Überwachung und Aufnahme des Telefonverkehrs für den Anschluß des Rechtsanwaltsbüros V. an. Begründet wurde der Beschluß damit, ein Mitarbeiter der Kanzlei sei verdächtig, eine um die Brüder Beker gebildete kriminelle Vereinigung zu unterstützen.

Weil der Ermittlungskomplex im Zusammenhang mit einem Verfahren stand, in dem das BKA früher bereits tätig geworden war, schaltete die Staatsanwaltschaft das BKA für die Durchführung der Abhörung ein.

Das BKA nahm u.a. auch ein Telefonat auf, das der Anwalt P. G. aus der Kanzlei V. mit dem Journalisten der Zeitschrift „Stern", Thomas Kettner, am 30. Januar 1990 um 15.18 Uhr führte.

Über dieses Gespräch fertigte das BKA am 30. Januar 1990 eine schriftliche Zusammenfassung und am 1. Februar 1990 ein vollständiges Wortprotokoll an.

Am 31. Januar 1990 überbrachte ein Mitarbeiter des BKA der Staatsanwaltschaft Frankfurt/M. eine Kopie der Zusammenfassung. Eine Abschrift des vollständigen Wortprotokolls erhielt die Staatsanwaltschaft einige Tage später.

Als der Mitarbeiter des BKA am 31. Januar 1990 der zuständigen Staatsanwältin die Zusammenfassung übergab, war ein Beamter des Kommissariats 53 des Frankfurter Polizeipräsidiums anwesend. Die Staatsanwältin informierte ihn bei dieser Gelegenheit über den Inhalt des abgehörten Telefonats. Das K 53 des Polizeipräsidiums in Frankfurt/M. leitet die Ermittlungen in dem Verfahren gegen die Brüder Beker. Nach Darstellung des K 53 erhielt es deshalb vom BKA später ebenfalls eine Kopie der Zusammenfassung. Dies sei mit Zustimmung der Staatsanwaltschaft geschehen. Die Staatsanwaltschaft schließt nicht aus, daß in der Tat eine Zustimmung erteilt wurde.

Kurz danach wurde die Polizeiabteilung im Innenministerium von der Kriminalabteilung des Polizeipräsidiums Frankfurt/M. über den Inhalt des abgehörten Telefongesprächs unterrichtet. Ende April 1990 forderte die Abteilung des Ministeriums die Zusammenfassung an und legte sie anschließend dem Minister vor. Aufgrund dieser Zusammenfassung fertigte der Minister einen Vermerk.

Diesen Vermerk hat der Minister am 24. Oktober 1990 in der Plenarsitzung des Hessischen Landtags verlesen. Er sagte dabei folgendes:

> „... Aber warum tun solche Menschen das? Ich weiß es nicht bei jedem, aber bei einer Person weiß ich das ganz genau: bei dem Journalisten Kettner. Das zeigt sein Gespräch mit einer mir namentlich bekannten Person in Frankfurt/M. über eine mögliche Äußerung Herrn Bekers. Kettner sagte, er sei nicht uninteressiert, man müsse nur einmal klären, was Herr Beker ihm erzählen wolle. Der Gesprächsteilnehmer erklärte, Beker werde sich doch nicht selbst belasten. Der Journalist wollte wissen, welche Politiker Geld bekommen hätten (...).
>
> Der Journalist meinte, der Preis sei natürlich sehr hoch, aber dann gerechtfertigt. Der Gesprächsteilnehmer: „Wenn Wallmann gehen muß danach"; lacht. Der Journalist: „So ist es, Sie haben es erfaßt." Der Gesprächsteilnehmer will noch einmal Rücksprache nehmen. Der Journalist will wissen, wer der und der sei. Entsprechende Aussagen gegen Wallmann seien einen erklecklichen Geldbetrag wert. Er kenne Beker persönlich, er habe bereits ein Gespräch mit ihm gehabt. Er betonte, daß die Zielrichtung eine politische sei. Als Gegenleistung für ein gehaltvolles Interview wird die Summe von 150.000 DM genannt ..."

Diese Äußerungen stimmen zum großen Teil wörtlich mit der Zusammenfassung des Telefonats überein.

3. Datenschutzrechtliche Bewertung

3.1
Anfertigen des Protokolls durch das Bundeskriminalamt im Auftrag der Staatsanwaltschaft Frankfurt/M.

Mit dem Beschluß des Amtsgerichts Frankfurt/M. vom 24. November 1989 lag die formale Voraussetzung für die Telefonüberwachungsmaßnahme der genannten Anschlüsse nach §§ 100a, 100b der Strafprozeßordnung vor.

Ich muß davon ausgehen, daß im vorliegenden Fall auch die materiell-rechtlichen Voraussetzungen für den richterlichen Beschluß gegeben waren.

3.2
Arbeitsablauf beim Bundeskriminalamt

Im Zuge der Überwachungsmaßnahmen nahm das Bundeskriminalamt am 30. Januar 1990 das Gespräch zwischen dem Journalisten Kettner und dem Anwalt auf.

Dazu ist folgendes zu erläutern: Die Polizei erfaßt bei Überwachungsmaßnahmen lediglich auf den Tonbändern lückenlos den gesamten Fernsprechverkehr des jeweiligen Anschlusses; in die formularmäßig aufbereiteten „Auswertungen" nimmt sie nur dann ausführliche Darlegungen auf, wenn auch ein Bezug zu den jeweiligen Ermittlungen gegeben ist. Bei reinen Privatgesprächen oder Inhalten ohne jede Verbindung mit der TÜ-Maßnahme werden lediglich Uhrzeit, soweit vorhanden Telefonnummer und Namen der Gesprächspartner vermerkt, nicht aber der Inhalt. Dieser wird allenfalls durch ein Prädikat (z.B. „privat") qualifiziert.

Ausführliche Wortprotokolle werden dann angefertigt, wenn dies notwendig erscheint. Im vorliegenden Fall wurden sowohl ein solches ausführliches Wortprotokoll wie auch eine zusammenfassende „Auswertung" erstellt.

Das erfaßte und ausgewertete Gespräch hatte keinen direkten Bezug zu den Ermittlungen, die zu dem Beschluß über die TÜ-Maßnahme geführt haben. Ob es sich somit um einen sogenannten „Zufallsfund", d.h. eine Information, die in bezug auf ein völlig anderes Ermittlungsverfahren oder einen anderen Sachverhalt von Bedeutung sein kann, handelt – so jedenfalls der ermittelnde Staatsanwalt – oder nicht, ist letztlich bedeutungslos. Jedenfalls betraf das Telefonat einen anderen Teil des gesamten Ermittlungskomplexes, der auch von einem anderen Dezernat in der StA Frankfurt/M. bearbeitet wird. Neben der für dieses Dezernat zuständigen Staatsanwältin erhielt auch das Kommissariat 53 des Polizeipräsidiums in Frankfurt/M. als ermittelnde Polizeidienststelle im Verfahren Beker eine zusammenfassende Auswertung, nicht aber das Wortprotokoll.

Nach Angaben des K 53 war für die Anforderung entscheidend, daß im Telefonat von „X" und „Y" die Rede war, sowie ein Betrag von DM 150.000 genannt wurde. Diese Buchstaben bzw. dieser Betrag seien früher bereits im Verfahren Beker erwähnt worden.

3.3
Bearbeitung der „Auswertung" der Telefonüberwachung und des Wortprotokolls durch die Staatsanwaltschaft in Frankfurt/M.

Nachdem die Beamten des Bundeskriminalamts das Telefongespräch zunächst als zusammenfassende Auswertung, später als Wortprotokoll niedergeschrieben hatten, waren sie verpflichtet, die Staatsanwaltschaft zu unterrichten. Die

§§ 100a, 100b StPO betonen ausdrücklich die Rolle der Staatsanwaltschaft als „Herrin des Verfahrens". Das Bundeskriminalamt wurde eingeschaltet, um die Bänder auszuwerten, während die übrigen Sachermittlungen im „Fall Beker" durch das Kommissariat 53 (K 53) des Frankfurter Polizeipräsidiums durchgeführt werden. Nach § 100a StPO sind Gegenstand und Betroffene der Telefonüberwachung genau im Text des richterlichen Beschlusses festgestellt. Ob die gewonnenen und schriftlich festgehaltenen Erkenntnisse erfaßt und weiterverarbeitet werden dürfen, muß deshalb von der Staatsanwaltschaft ständig überprüft werden. Dies ergibt sich ohne weiteres aus § 100b, Abs. 4 und 5 StPO, wonach bei Wegfall der Voraussetzungen des § 100a die Überwachungsmaßnahmen sofort zu beenden und gemäß Abs. 5 die nicht mehr zur Strafverfolgung erforderlichen Unterlagen unter Aufsicht der Staatsanwaltschaft zu vernichten sind. Sinn dieser Verpflichtung der Staatsanwaltschaft, bei der Vernichtung anwesend zu sein, ist es, daß diese den Umfang der Aussonderung bestimmt, „damit nicht aus übergroßer Vorsicht zuwenig vernichtet wird, andererseits aber auch, damit alles Beweiserhebliche erhalten bleibt" (Schäfer in: Löwe/Rosenberg, Kommentar zur StPO, 24. Auflage, § 100b Randnr. 9a).

Die zuständige Staatsanwältin hat ca. acht Monate die Unterlagen in ihrem Schreibtisch aufbewahrt. Nach ihren Äußerungen hatten die Unterlagen zum Zeitpunkt der Übergabe im Februar 1990 noch keine eindeutige Verfahrensrelevanz, d.h. sie fügten sich nicht mit den übrigen Informationen im Verfahren Beker so zu einem Bild zusammen, daß sie eindeutig für den weiteren Gang des Ermittlungsverfahrens von Bedeutung sein würden.

In der Tat spricht vieles dafür, daß diese Informationen keine direkte strafrechtliche Relevanz besitzen. Jedenfalls hätte im Zeitraum von acht Monaten eine endgültige Entscheidung – Vernichtung oder Einfügung in die Sachakte im Verfahren Beker – getroffen werden müssen. § 100b Abs. 4 und 5 StPO verlangen eine ständige Prüfung der Erforderlichkeit und bei negativem Ausgang wenigstens eine „alsbaldige" Vernichtung (Kleinknecht/Meyer, Strafprozeßordnung, Kommentar, Randnr. 7 zu § 101; noch strenger Müller in: Kleinknecht/Müller/Randberger (KMR) Kommentar zur StPO, Anmerkung 11 zu § 101, der eine sofortige Vernichtung verlangt).

Selbst wenn die Aufbewahrung der Unterlagen im Schreibtisch der Staatsanwältin als ihre Entscheidung gewertet würde, daß damit die Schriftstücke verfahrensrelevant sind, hätten diese keinesfalls an diesem Ort aufbewahrt werden dürfen. Im Strafprozeß gilt aus Gründen der Rechtsklarheit und Rechtssicherheit der Grundsatz der Vollständigkeit der Akte.

3.4
Weiterleitung an das K 53 und das Hessische Ministerium des Innern

Das Bundeskriminalamt unterrichtete die ermittelnde Dienststelle K 53 im Polizeipräsidium „vorab" noch am Tage der Aufnahme des Telefongesprächs. Hiervon wußte die Staatsanwaltschaft nichts. Am nächsten Tag erhielt das K 53 die zusammengefaßte „Auswertung" möglicherweise mit Zustimmung der Staatsanwaltschaft von Beamten des BKA. Noch am gleichen Tage gab das K 53 eine Kopie der zusammengefaßten Niederschrift an seine Abteilungsleitung weiter. Wiederum am gleichen Tag teilte diese der Polizeiabteilung im Innenministerium den Inhalt des Gesprächs mit und übergab ihr drei Monate später, am 30. April 1990, die zusammengefaßte „Auswertung" des Telefongesprächs.

Von der polizeiinternen Verwendung der Unterlagen erfuhr die Staatsanwaltschaft nichts.

Die Polizei rechtfertigt diese Übermittlung damit, daß die Vorabinformation des K 53 durch das BKA im Rahmen des „fast täglich durchgeführten Informationsaustausches" vorgenommen worden sei.

Die Weitergabe innerhalb des Polizeipräsidiums in Frankfurt/M. wurde mit beamtenrechtlichen Vorschriften (§ 70 HBG), einer in diesem Verfahren angeordneten besonderen Berichtspflicht und dem allgemeinen Loyalitätsprinzip begründet.

Zur Rechtfertigung der Weiterleitung an das Ministerium berufen sich die Polizeidienststellen auf folgende Rechtsvorschriften:

1. Die §§ 58 ff. HSOG, insbesondere § 59, der die Dienst- und Fachaufsicht des Innenministeriums über die Polizeidienststellen begründet.

2. § 3 Abs. 3 der Polizeiorganisationsverordnung, der die Polizeidienststellen verpflichtet, die zuständigen Aufsichtsbehörden unverzüglich über alle wichtigen Vorgänge zu unterrichten und

3. in Konkretisierung dieser Vorschrift der sogenannte „WE-Erlaß", der die Dienststellen der Vollzugspolizei verpflichtet, „über wichtige Ereignisse in vollzugspolizeilichen Angelegenheiten" zu berichten (Staatsanzeiger 1986 S. 23). In letztgenanntem Erlaß werden eine Reihe von Ereignissen genannt, die in jedem Fall eine Berichtspflicht gegenüber den vorgesetzten Behörden begründen. Dazu gehören auch gemäß Ziff. 2.9 strafbare Handlungen und Vorkommnisse sonstiger Art, die (u.a.) Persönlichkeiten oder Institutionen des öffentlichen Lebens berühren.

Die Fachabteilung III im Hessischen Ministerium des Innern (Polizei) verweist darüber hinaus auf

- den engen Zusammenhang der beiden Ermittlungsverfahren,
- den Umstand, daß in beiden Komplexen Bedienstete öffentlicher Stellen in dringendem Verdacht standen, Amtsdelikte begangen zu haben,
- die strafrechtlich relevante Verwicklung auch von Polizeibeamten in einem der beiden Ermittlungskomplexe,
- die Tatsache, daß auf noch unbekannten Wegen Ermittlungsunterlagen Teilen der Medien zugänglich gemacht worden waren,
- sowie ein aktuell zu erwartendes großes Medieninteresse bezüglich beider Ermittlungskomplexe.

Angesprochen auf die Frage, unter welchen Umständen Angaben aus einer Telefonüberwachung weitergegeben werden dürfen, erklärten hingegen der Leiter der Staatsanwaltschaft Frankfurt/M. ebenso wie der ermittelnde Staatsanwalt im Verfahren V., in solchen Fällen dürften Informationen durch die unmittelbar ermittelnden Polizeidienststellen nur dann weitergeleitet werden, wenn die Staatsanwaltschaft ihr Einverständnis erklärt hat. Der zuständige Dezernent erklärte darüber hinaus, dies sei seiner Ansicht nach auch die vom BKA geübte Praxis.

Bei der datenschutzrechtlichen Bewertung, ob die im Rahmen der Telefonüberwachung gewonnenen Informationen bzw. Schriftstücke weitergegeben werden durften, ist von zwei Grundsätzen auszugehen: der Erforderlichkeit und der Zweckbindung.

Soweit insbesondere das K 53 Informationen bzw. ein Schriftstück erhielt, um damit das eigene Ermittlungsverfahren zu fördern, bestehen keine Einwände gegen diese Übermittlung.

Problematisch bleibt jedoch die Tatsache, daß das K 53 die Vorabinformation durch das BKA ohne vorheriges Einverständnis der Staatsanwaltschaft erhielt. Diese war die zuständige ermittelnde Behörde und hätte deshalb die Entscheidung über die Verwendung der Unterlagen treffen müssen.

Soweit das Ministerium des Innern feststellt, es habe sowohl die Information wie auch die zusammengefaßte „Auswertung" aus fachaufsichtlichen Gründen erhalten müssen, ist festzustellen:

Die §§ 160 ff. der Strafprozeßordnung und § 152 GVG gehen davon aus, daß die Polizeibeamten als Hilfsbeamte der Staatsanwaltschaft tätig sind. Sie unterstehen damit grundsätzlich der Fachaufsicht des Staatsanwaltes.

Es ist zwar richtig, daß in der Mehrzahl aller Ermittlungsverfahren die Polizei selbständig und zunächst ohne Einwirkung der Staatsanwaltschaft das Ermittlungsverfahren führt und auch abschließt. In diesen Fällen mag dahingestellt bleiben, ob und inwieweit die Fachaufsichtsbehörden der Kriminalpolizei in diese Ermittlungstätigkeit eingreifen können.

Wenn jedoch die Staatsanwaltschaft ausdrücklich das Ermittlungsverfahren selbst führt, sind fachaufsichtliche Maßnahmen durch vorgesetzte Polizeidienststellen nicht mehr zulässig. Jede andere Interpretation würde die Gefahr konkurrierender fachaufsichtlicher Maßnahmen von Staatsanwaltschaft und vorgesetzten Polizeidienststellen in sich bergen.

Noch deutlicher ist die Rechtslage dann, wenn eine Telefonüberwachung nach §§ 100a, 100b StPO durchgeführt wird.

Nach § 100b Abs. 1 StPO kann eine solche Maßnahme nur unter Beteiligung der Staatsanwaltschaft getroffen werden. Bei Gefahr im Verzug kann sie eine Anordnung für den Zeitraum von drei Tagen treffen, die dann jedoch von dem zuständigen Richter bestätigt werden muß. Ausdrücklich und im Gegensatz zu anderen Maßnahmen nach der Strafprozeßordnung gesteht das Gesetz den Hilfsbeamten keine sogenannte „Eilkompetenz" zur Durchführung dieser Maßnahme zu.

Darin liegt eine bewußte Entscheidung des Gesetzgebers, der auch in den weiteren Bestimmungen des § 100b StPO die Sachleitungsbefugnis der Staatsanwaltschaft ausdrücklich betont. Dies gilt insbesondere für die nach Abs. 4 anzuordnende unverzügliche Beendigung der TÜ-Maßnahme, wenn die Voraussetzungen nach § 100a StPO nicht mehr vorliegen, etwa wenn der Tatverdacht entkräftet oder die Maßnahme nicht mehr unentbehrlich oder nicht mehr aussichtsreich ist (Kleinknecht/Meyer, Kommentar zur Strafprozeßordnung, 37. Auflage, § 100b Randnr. 6). Nach § 100b Abs. 5 StPO sind die erlangten Unterlagen, soweit nicht mehr erforderlich, „unter Aufsicht der Staatsanwaltschaft zu vernichten". Auch dieses Gebot ist keineswegs der Regelfall nach der StPO, sondern bildet eine Ausnahme, die die Schwere des Grundrechtseingriffs unterstreicht, der mit der Überwachung und Aufnahme des Fernmeldeverkehrs im Strafverfahren verbunden ist.

Soweit wegen der möglichen Verwicklung von Polizeibeamten in die Beker-Affäre dienstaufsichtliche Gründe für die Weiterleitung der Unterlagen angeführt werden, kann ich keinerlei Zusammenhang mit dem Inhalt des abgehörten Telefonats erkennen. Insbesondere sehe ich keinen Anhaltspunkt dafür, daß die in dem Gespräch erwähnte Summe von DM 150.000 in irgendeiner Verbindung zu einem disziplinarrechtlichen Sachverhalt stehen soll.

Soweit das allgemeine große Medieninteresse am Ermittlungsverfahren V. als Begründung für die Notwendigkeit der Übermittlung an das Ministerium genannt wurde, ist festzustellen: Ein solches Interesse kann auf keinen Fall eine Übermittlung von Informationen aus einer Telefonüberwachung rechtfertigen.

3.5
Weiterleitung der Informationen bzw. der zusammenfassenden „Auswertung" im Ministerium des Innern an Minister Milde

Minister Milde war Dienstvorgesetzter der Mitarbeiter in der Fachabteilung Polizei seines Hauses. Was den Mitarbeitern dienstlich bekannt wird, darf auch an den Minister als unmittelbaren Vorgesetzten weitergeleitet werden.

3.6
Unterrichtung der Staatsanwaltschaft und Umsetzung des Vernichtungsgebots

Wie bereits ausgeführt, ist zumindest die Vorabinformation des K 53 durch die Ermittlungsabteilung des BKA sowie die weitere Benachrichtigung der vorgesetzten Dienststellen von K 53, insbesondere des Ministeriums des Innern, ohne Zustimmung der Staatsanwaltschaft erfolgt.

Die Staatsanwaltschaft in Frankfurt/M. vertritt die Auffassung, daß ihre Zustimmung in jedem Fall eingeholt werden müsse und dies in der Praxis auch der Fall sei.

Verzichtet man darauf, daß die Unterlagen jeweils nur mit Kenntnis der Staatsanwaltschaft weitergegeben werden können, so verzichtet man auch auf deren Kenntnis, wo sich die Unterlagen im einzelnen befinden. Niemand würde dafür Sorge tragen, daß Empfänger, die durchaus auch auf rechtmäßigem Wege diese Unterlagen erhalten haben, über die Vernichtung und ihre Gründe unterrichtet werden. Damit wäre die Wahrscheinlichkeit groß, daß dort Unterlagen weiter existieren und die eigentliche Vernichtung unter Aufsicht der Staatsanwaltschaft einen großen Teil ihrer Wirkung verliert. Aus der Sicht des Betroffenen wäre dies geradezu unerträglich.

Mit anderen Worten: § 100b Abs. 5 StPO liefe leer, wenn die Staatsanwaltschaft nicht ausdrücklich benachrichtigt würde, sofern Angaben aus der Telefonüberwachung einem anderen Zweck zugeführt werden sollen.

3.7
Verwendung der Auswertung der Telefonüberwachung durch Minister Milde im Plenum des Hessischen Landtags

Minister Milde hat dargelegt, daß er zum Schutz der Ehre des Ministerpräsidenten in einer Rechtsgüterabwägung zu dem Ergebnis gekommen sei, die Rechtmäßigkeit einer Weitergabe von Erkenntnissen aus der Telefonüberwachung an das Plenum sei zu bejahen. Ganz gleich, wie man die Weitergabe der Informationen an den Minister bewertet, kann das Argument der Rechtsgüterabwägung nicht die rechtliche Zulässigkeit der Weitergabe begründen. Die Erkenntnisse aus der Telefonüberwachung durften nur zweckgebunden, und daher nicht in der Debatte im Landtag verwendet werden.

Eine Telefonüberwachung ist ein Eingriff in das in Art. 10 GG geschützte Fernmeldegeheimnis, dem das Grundgesetz einen hohen Rang zuweist (BVerfGE 67, 157, 171). Gemäß Art. 10 Abs. 2 GG darf der Eingriff nur aufgrund eines Gesetzes erfolgen. Der Grundsatz der Verhältnismäßigkeit muß gewahrt sein. Die Überwachungsmaßnahmen müssen auf das unumgänglich Notwendige beschränkt werden (BVerfGE 30, 1, 22). Im Hinblick auf den Grundsatz der Verhältnismäßigkeit begrenzen die §§ 100a, 100b StPO die Zulässigkeit eines Eingriffs in das Fernmeldegeheimnis ausschließlich auf die Verfolgung bestimmter, besonders schwerwiegender Straftaten. Ferner legt § 100b Abs. 5 StPO fest, daß die durch die Überwachungsmaßnahmen erlangten Unterlagen unter Aufsicht der Staatsanwaltschaft zu vernichten sind, wenn sie für die Strafverfolgung nicht mehr erforderlich sind.

Die durch eine Telefonüberwachung gewonnenen Erkenntnisse dürfen nur strikt zweckgebunden verwendet werden: Zum einen stellt § 100b Abs. 5 StPO für die Frage der Erforderlichkeit der (weiteren) Verwendung der Unterlagen eindeutig klar, daß der Zweck der Strafverfolgung allein maßgebend ist. Zum anderen würden auch die konkreten in § 100a StPO festgelegten rechtlichen Begrenzungen einer Telefonüberwachung weitgehend leerlaufen, wenn die bei einer Telefonüberwachung gewonnenen Erkenntnisse zu anderen Zwecken weiterverwendet würden, die eine Telefonüberwachung als Maßnahme zur Erhebung von Daten nicht zulassen. Schließlich könnte die Staatsanwaltschaft ihrer in § 100b Abs. 5 StPO niedergelegten Verpflichtung, nicht (mehr) erforderliche Informationen zu vernichten, nicht nachkommen, wenn in der Zwischenzeit diese Unterlagen an weitere Stellen gelangen und dort wiederum weiterverarbeitet werden bzw. der mit dieser Verpflichtung der Staatsanwaltschaft beabsichtigte Schutz der von der Überwachung Betroffenen würde nicht erreicht.

Mit der besonderen Konstellation der Verwendung von Erkenntnissen aus einer Telefonüberwachung zu parlamentarischen Zwecken hat sich das Hamburgische Verfassungsgericht 1988 befaßt (NJW 1989, 1081). Hier ging es um die Frage, ob der Parlamentarische Untersuchungsausschuß „Hafenstraße" über die staatsanwaltschaftlichen Ermittlungsakten hinaus auch aus der Telefonüberwachung gewonnene Unterlagen erhalten darf. Das Verfassungsgericht geht davon aus, daß der Eingriff in das Fernmeldegeheimnis nicht lediglich im Vorgang des Abhörens und Aufzeichnens von Telefongesprächen liegt, sondern gleichermaßen in der Auswertung von Aufzeichnungen. Es geht um den Schutz des Inhalts der Gespräche. Demzufolge hat das Gericht in der Vorlage der Unterlagen an den Untersuchungsausschuß einen neuen Eingriff in das Fernmeldegeheimnis gesehen, der einer besonderen Rechtsgrundlage bedarf. Da eine solche gesetzliche Grundlage nicht vorlag, hat das Gericht die Zulässigkeit einer Vorlage der Erkenntnisse aus der Telefonüberwachung an den Parlamentarischen Untersuchungsausschuß verneint.

Auch die Verwendung der Erkenntnisse aus der Telefonüberwachung von Minister Milde für die politische Auseinandersetzung im Plenum des Hessischen Landtags sehe ich als erneuten Eingriff in das Fernmeldegeheimnis an, für den es einer besonderen gesetzlichen Grundlage bedurft hätte. Eine solche gesetzliche Vorschrift liegt nicht vor. Grundsätzlich muß jeder Bürger mit der Möglichkeit rechnen, daß er bei einem Telefongespräch – als Beschuldigter oder als unbeteiligter Dritter – ohne sein Wissen abgehört wird. Er muß deshalb darauf vertrauen können, daß die auf diese Weise gewonnenen Erkenntnisse nur in der gesetzlich festgelegten Weise verwendet werden und nicht in einem völlig anderen Zusammenhang von staatlichen Instanzen benutzt werden.

Es kommt auch nicht darauf an, ob von Minister Milde ausdrücklich darauf hingewiesen wurde, daß die wiedergegebenen Informationen durch eine Telefonüberwachung gewonnen wurden. Entscheidend ist, daß durch das Fernmeldegeheimnis der Inhalt des Gesprächs geschützt wird. Ebensowenig ist es von Bedeutung, ob nur ein Teil des Gesprächs wiedergegeben wurde oder ob das Gespräch wörtlich zitiert wurde.

4. Weitere Konsequenzen

Dieser Bericht und die ihm zugrundeliegenden Vorgänge thematisieren nachdrücklich die Gesamtproblematik der Aufbewahrung von Bändern und schriftlichen Unterlagen aus Abhörmaßnahmen sowie deren Verwendung und Weitergabe außerhalb des strafrechtlichen Ermittlungsverfahrens. Meines Erachtens sind – in Stichworten zusammengefaßt und ohne Anspruch auf Vollständigkeit – zunächst folgende Schritte und Aktivitäten erforderlich:

a) Im Ministerium des Innern sind, soweit sie nicht für die staatsanwaltschaftlichen Ermittlungen benötigt werden bzw. zu diesem Zweck ausgehändigt werden müssen, die Dokumente betr. die Aufzeichnung des Telefonats vom 30. Januar 1990 umgehend zu vernichten.

b) Es muß in geeigneter Weise, etwa durch Erlaß, gegenüber Polizeibeamten, die gleichzeitig als Hilfsbeamte der Staatsanwaltschaft fungieren, klargestellt werden, daß sie in bezug auf die Handhabung und Weiterleitung von Unterlagen aus Aufzeichnungen des Fernmeldeverkehrs nach §§ 100a, 100b StPO grundsätzlich den Anordnungen des zuständigen Staatsanwalts unterliegen, und zwar auch im Verhältnis zu den vorgeordneten Polizeidienststellen einschließlich des Ministeriums des Innern.

c) Zu klären ist weiterhin, wie das BKA mit den aus Telefonüberwachungsmaßnahmen gewonnenen Erkenntnissen in den Fällen verfahren muß, in denen es von hessischen Staatsanwaltschaften eingeschaltet wurde.

d) Der Vollzug des Vernichtungs- bzw. Löschungsgebots des § 100b Abs. 5 StPO ist bei allen beteiligten Stellen zu überprüfen. Dies gilt zum einen für die in den Räumen der Staatsanwaltschaft selbst asservierten Bänder und in die Akten aufgenommenen Aufzeichnungen. Dies gilt weiter für die Behörden, die für die Staatsanwaltschaften Maßnahmen der Überwachung des Fernmeldeverkehrs durchführen, also insbesondere das Landes- und das Bundeskriminalamt.

   Wichtig ist dabei für mich vor allem zu klären,

   – zu welchem Zeitpunkt die Staatsanwaltschaften die Entscheidung darüber treffen, daß die Unterlagen zur Strafverfolgung nicht mehr erforderlich sind,

   – wann und wie diese Entscheidungen an die in die TÜ-Maßnahmen eingeschalteten Polizeidienststellen gelangen und

   – wie sichergestellt wird, daß alle Bänder und Unterlagen einschließlich der zwischenzeitlich gefertigten Kopien und Abschriften gelöscht bzw. vernichtet werden.

e) Die Verwendung des Abhörprotokolls innerhalb des Bundeskriminalamts ist nach meiner Auffassung zu überprüfen. Soweit das BKA von den unter a bis d aufgeführten Punkten betroffen ist, werde ich den Bundesbeauftragten bitten, die entsprechenden Feststellungen zu treffen. Der Bundesbeauftragte hat bereits erste Gespräche im BKA geführt.

17.2.2
Bericht der Landesregierung vom 14. November 1990 zu dem Beschluß des Hauptausschusses vom 8. November 1990 betreffend den Umgang mit Informationen, die aus Telefonüberwachungsmaßnahmen gewonnen wurden, innerhalb der Landesregierung

Der Hauptausschuß hat in seiner Sitzung vom 8. November 1990 folgenden Beschluß gefaßt:

> Die Landesregierung wird um einen Bericht über den Umgang mit Informationen, die aus Telefonüberwachungsmaßnahmen gewonnen wurden, innerhalb der Landesregierung ersucht, der dem Ausschuß in Verbindung mit einer Stellungnahme des Datenschutzbeauftragten vorgelegt werden soll.

Gemäß diesem Beschluß berichte ich als derzeit mit der Wahrnehmung der Aufgaben des Hessischen Ministeriums des Innern beauftragter Minister für die Landesregierung wie folgt:

A.
Wegen des Sachverhalts, der die Anordnung der in Rede stehenden Telefonüberwachungsmaßnahme, deren Durchführung und die Weiterleitung durch das Bundeskriminalamt an die Staatsanwaltschaft in Frankfurt am Main, die Kriminalpolizei in Frankfurt am Main und von dort an das Hessische Ministerium des Innern betrifft, nehme ich bezug auf den Bericht des Hessischen Datenschutzbeauftragten, den dieser am 8. November 1990 dem Hauptausschuß vorgelegt hat. Wie der Hessische Datenschutzbeauftragte in diesem Bericht ausgeführt hat, sind ihm bei seiner Überprüfung zur Aufklärung des Sachverhalts „von sämtlichen beteiligten hessischen Stellen alle erforderlichen Dokumente zur Verfügung gestellt und alle gewünschten Auskünfte erteilt worden". Die von dem Datenschutzbeauftragten hierauf getroffenen Feststellungen ensprechen – soweit sie den Sachverhalt betreffen – den Erkenntnissen der Landesregierung.

B.
Über den weiteren Umgang mit Informationen, die aus der in Rede stehenden Telefonüberwachungsmaßnahme gewonnen wurden, hat mir der Chef der Staatskanzlei wie folgt berichtet:

„I. Nach Kenntnis des Chefs der Staatskanzlei hat kein Angehöriger dieser Behörde vor der Rede Staatsminister Mildes im Landtag am 24. Oktober 1990 Kenntnis von der Tatsache eines Abhörvorgangs und dessen eventueller öffentlicher Verwendung gehabt.

II. 1. Etwa Ende Juni/Anfang Juli hat der Innenminister den Chef der Staatskanzlei bei Gelegenheit einer Landtagssitzung mündlich davon informiert, daß der „STERN" mit unlauteren Mitteln aus politischen Gründen angeblich belastendes Material gegen den Hessischen Ministerpräsidenten zusammenstellen würde. Der Minister erwähnte, daß dabei „viel Geld" im Spiele sei und daß es sich um denselben Komplex wie im Fall des V-Mannes handele. Ob dabei der Name Thomas Kettner fiel, ist dem Chef der Staatskanzlei nicht mehr erinnerlich. Die anderen Namen, die später in der Presseerklärung des STERN auftauchten, fielen nicht. Der Innenminister lehnte es ausdrücklich ab, die Herkunft seines Wissens offenzulegen.

Zu diesem Zeitpunkt war dem Chef der Staatskanzlei durch den Innenminister bekannt, daß ein Informant der Polizei bei einer Vernehmung die Behauptung aufgestellt hatte, daß er Beker und seine Freundin einmal zu dem früheren Oberbürgermeister in dessen Frankfurter Wohnung gefahren habe. Er hatte darüber auch telefonisch mit dem Frankfurter Polizeipräsidenten gesprochen, der aus Gründen der Sicherheit des V-Mannes eine Klärung der mit seinen sonstigen Aussagen nicht in Zusammenhang stehenden Behauptungen abgelehnt hatte. Außerdem war dem Chef der Staatskanzlei zu diesem Zeitpunkt privat bekannt, daß der STERN-Journalist Thomas Kettner im weiteren Bekanntenkreis des früheren Frankfurter Oberbürgermeisters nach Belegen für die Behauptung suchte, Beker habe Oberbürgermeister Wallmann privat getroffen. Aufgrund dieser Informationen rief der Chef der Staatskanzlei Anfang Juli den ihm aus dem Bundespresseamt persönlich bekannten Chefredakteur des STERN Schmidt-Holtz an und trug ihm seine Sorge vor, daß nach seinen Informationen von Mitarbeitern des STERN versucht werde, mit unlauteren Mitteln, d.h. unter Einsatz von Geld, aus politischen Gründen angeblich belastendes Material gegen den Hessischen Ministerpräsidenten zusammenzustellen. Der Chef der Staatskanzlei wies Herrn Schmidt-Holtz darauf hin, daß es sich bei allen sogenannten Beweisen über angebliche Beziehungen Wallmann- Beker nur um Falschinformationen handeln könne und bat ihn, sich dieses „Material" genau anzusehen. Der Chefredakteur des STERN sagte dies zu, da er nicht die Absicht habe, sein Organ Fälschungen zu öffnen.

Der Chef der Staatskanzlei informierte über dieses Gespräch weder den Ministerpräsidenten noch den Innenminister. Da dem Ministerpräsidenten die Angaben des V-Mannes bekannt waren, wollte er ihn nicht zusätzlich mit seinem Wissen über mögliche weitere Falschbehauptungen belasten.

II. 2. Zur Vorbereitung der Aktuellen Stunde über die Veröffentlichung der Behauptung des V-Mannes in BILD Frankfurt am 20. Oktober hat es mehrere Gespräche und telefonische Kontakte zwischen dem Ministerpräsidenten und dem Chef der Staatskanzlei einerseits und dem Chef der Staatskanzlei und dem Innenminister sowie dem Frankfurter Polizeipräsidenten andererseits gegeben. Erschwert wurden diese Kontakte durch den Besuch Minister Mildes mit dem Hauptausschuß in Budapest und die anschließende Krankheit des Ministers.

Nachdem der V-Mann sich offensichtlich selbst enttarnt hatte oder durch rechtswidrige Aktenpreisgabe enttarnt worden war, war es das Ziel des Ministerpräsidenten, die Behauptungen sofort aufklären zu lassen. Zu diesem Zweck wurde zwischen dem Innenminister und dem Chef der Staatskanzlei eine weitere Befragung des V-Mannes besprochen, deren Ergebnis der Innenminister als Vermerk dem Chef der Staatskanzlei am 22. Oktober von seinem Haus zustellen ließ. Aus diesem Befragungsvermerk ergaben sich Fragen hinsichtlich der Form und des Umfanges der Bewachung des Hauses des früheren Oberbürgermeisters zum Zeitpunkt des behaupteten Beker-Besuches. Am Nachmittag des 22. Oktober fand deshalb ein Gespräch zwischen dem Innenminister und dem Chef der Staatskanzlei, der vom Büroleiter des Ministerpräsidenten begleitet wurde, im Privathaus des Innenministers in Darmstadt statt. Dabei ging es um Widersprüche zwischen der ersten, dem Chef der Staatskanzlei nicht im Detail bekannten Aussage des V-Mannes und seiner neuen Einlassung. Zu diesem Gespräch kam der Ministerpräsident hinzu, der auf der Fahrt von einem Redaktionsgespräch beim Darmstädter Echo zur Regionalkonferenz Südhessen war. In seiner Begleitung befanden sich der Regierungssprecher und der Sprecher der CDU-Fraktion. Nachdem noch einmal ausführlich die durch zusätzliche telefonische Informationen des Frankfurter Polizeipräsidenten über die Art der Bewachung des Hauses Nasenring 30 erhärteten Widersprüche in den Behauptungen des V-Mannes erörtert worden waren, erwähnte der Minister, daß ihm Informationen vorlägen, wonach der STERN-Journalist Thomas Kettner 150.000 DM für belastendes Material im Zusammenhang mit den Behauptungen des V-Mannes geboten habe. Der Minister nannte weder die Quelle noch Einzelheiten. Er bejahte allerdings auf Nachfrage des Chefs der Staatskanzlei, daß es sich hierbei um die gleichen Informationen handele, die er Ende Juni/Anfang Juli von ihm erhalten habe. Auf die Frage des Ministerpräsidenten, ob der Innenminister diese Informationen verwenden könne und dies auch tun werde, entgegnete der Innenminister, daß er diese Informationen verwenden könne, aber noch nicht wisse, ob, wie und wann er dies tue.

Mit diesem Gespräch endet die Befassung des Chefs der Staatskanzlei und der angesprochenen Mitarbeiter der Staatskanzlei mit dieser Frage.

Der Chef der Staatskanzlei hat selbst weder an der Fraktionsvorstandssitzung noch an der Fraktionssitzung vom 23. Oktober teilgenommen.

Nach Auskunft des Sprechers der Landesregierung ist diese Thematik in der Fraktionssitzung weder vom Ministerpräsidenten noch vom Innenminister angesprochen worden. An der Fraktionsvorstandssitzung hat keiner der Genannten teilgenommen."

Der Ministerpräsident hat mir mitgeteilt, daß der dargestellte Verlauf des Gesprächs am 22. Oktober 1990, soweit er ihn betreffe, auch seiner Erinnerung entspreche. Der Sprecher der Landesregierung und der Leiter des persönlichen Büros des Ministerpräsidenten haben nachstehende dienstliche Erklärungen abgegeben.

„Dienstliche Erklärung

Ich habe den Bericht des Chefs der Staatskanzlei vom 13. November dieses Jahres zur Kenntnis genommen und erkläre, daß der darin dargestellte Sachverhalt, soweit ich Kenntnis davon habe, auch meiner Erinnerung entspricht.

Ich erkläre darüber hinaus, daß kein(e) andere(r) Mitarbeiter(in) der Abteilung Information mit dem im Bericht dargestellten Sachverhalt befaßt war."

„Dienstliche Erklärung

Die Darstellung in dem Bericht des Chefs der Staatskanzlei vom 13. November 1990 entspricht, soweit ich Kenntnis von dem Sachverhalt habe, auch meiner Erinnerung.

Andere Mitarbeiter des Persönlichen Büros waren mit dem im Bericht dargestellten Sachverhalt nicht befaßt."

C.
Für den Geschäftsbereich des Hessischen Ministeriums des Innern hat der Staatssekretär beim Hessischen Ministerium des Innern folgende Stellungnahme abgegeben:

„Wie sich aus dem Bericht des Datenschutzbeauftragten vom 8. November 1990 bereits ergibt, ist die schriftliche Zusammenfassung über das vom BKA abgehörte Telefongespräch direkt vom zuständigen Referenten des Hessischen Ministeriums des Innern an Herrn Staatsminister Milde geleitet worden. Von der Existenz dieser schriftlichen Zusammenfassung habe ich von Herrn Staatsminister Milde am 23. Oktober 1990 erfahren. Ich habe keine Einsicht in diese schriftliche Zusammenfassung genommen. Auch den Inhalt dieser Zusammenfassung habe ich nicht erfahren. Der der schriftlichen Zusammenfassung zugrundeliegende Sachverhalt ist mir erst durch die Rede von Herrn Staatsminister Milde im Landtag am 24. Oktober 1990 bekanntgeworden."

Der Pressesprecher des Hessischen Ministeriums des Innern hat in einer Stellungnahme vom 12. November 1990 niedergelegt, daß er keine Kenntnis der in Rede stehenden schriftlichen Zusammenfassung der Telefonüberwachung gehabt habe. Auch der dieser Zusammenfassung zugrundeliegende Sachverhalt sei ihm erst durch die Rede von Staatsminister Milde am Mittwoch, dem 24. Oktober 1990, im Plenum des Hessischen Landtages bekanntgeworden.

Weitere Einzelheiten im Zusammenhang mit der Presseerklärung des Hessischen Ministeriums des Innern vom 24. Oktober 1990 ergeben sich aus seiner als Anlage zu diesem Bericht beigefügten Stellungnahme.

(Koch)
Staatsminister

Anlage

Christian Jaletzke

Wiesbaden, den 12. November 1990

– M 2 –
Referat M 3

im Hause

Bericht der Landesregierung gemäß Beschluß des Hauptausschusses des Hessischen Landtages vom 8. November 1990
hier: Stellungnahme

1. Ich hatte keine Kenntnis der in Rede stehenden schriftlichen Zusammenfassung der Telefonüberwachung. Auch der dieser Zusammenfassung zugrundeliegende Sachverhalt ist mir erst durch die Rede von Herrn Milde am Mittwoch, dem 24. Oktober 1990, im Hessischen Landtag bekanntgeworden.

2. Am Mittwoch, dem 24. Oktober 1990, war ich seit Beginn der Plenardebatte des Hessischen Landtages auf der Referententribüne anwesend. Während der Rede von Herrn Milde sprachen mich mehrere Journalisten daraufhin an, ob sie von mir den Redetext von Herrn Milde erhalten könnten. Da ich kein Redemanuskript besaß, nicht wußte, ob es überhaupt ein Redemanuskript gab und auch nicht den Inhalt der Rede kannte, konnte ich diesen Bitten und Nachfragen nicht entsprechen. Daraufhin wurde ich gefragt, ob es denn wenigstens eine Pressemitteilung des Hessischen Ministeriums des Innern geben werde. Aufgrund der Anfragen der Journalisten entschloß ich mich – mit Herrn Milde bestand nicht die Möglichkeit einer Rücksprache hierzu –, nach Beendigung der Rede von Herrn Milde eine Pressemitteilung zu schreiben.

   Bereits während der Rede von Herrn Milde mußte ich mehrfach an das hinter der Referententribüne befindliche Telefon gehen. Ferner mußte ich auch für Anrufe meiner Mitarbeiter aus der Pressestelle des Ministeriums erreichbar bleiben. Ich bat deshalb einen Mitarbeiter der CDU-Fraktionsgeschäftsstelle, mir eine kurze Zusammenfassung der wichtigsten Redeteile der soeben beendeten Rede von Herrn Milde zu erstellen. Nachdem der Fraktionsmitarbeiter diese Zusammenfassung geschrieben hatte, wurde sie mir von ihm ausgehändigt.

   Aus dieser erbetenen Zusammenfassung heraus habe ich dann in der CDU-Fraktionsgeschäftsstelle eine Pressemeldung diktiert, da ich aus Zeitgründen nicht erst ins Innenministerium zurückfahren konnte, denn die Pressemitteilung sollte natürlich baldmöglichst an die auf der Pressetribüne wartenden Journalisten verteilt werden, die längst schon die Pressemitteilung der CDU zur Rede von Herrn Nassauer in Händen hatten.

   Die Überschrift und den entsprechenden Passus in dieser Pressemitteilung bezüglich möglicher Ministerpräsident Dr. Wallmann belastender Äußerungen habe ich so formuliert, wie ich es glaubte, in der Rede von Herrn Milde verstanden zu haben.

   Die Pressemitteilung wurde sodann kopiert und unverzüglich an die wartenden Journalisten verteilt. Die Pressemitteilung wurde dann an meine Mitarbeiter in der Pressestelle des Innenministeriums gefaxt und von dort aus per Telefax an den Presseverteiler des Innenministeriums weitergegeben. Gleichfalls erfolgte eine Versendung an die Bezieher des Postverteilers. Auch die CDU-Fraktionsgeschäftsstelle hat, wie ich später erfahren habe, die Meldung an verschiedene Journalisten gefaxt. Nach wie vor hatte ich keine Rücksprache mit Herrn Milde.

3. Behauptungen wie z.B. in der Süddeutschen Zeitung vom 9. November 1990, Milde habe „seinen Verstoß gegen das Daten- und Strafrecht vorher über seine Pressestelle ankündigen lassen" sind – soweit sie sich auf die Pressestelle des Hessischen Innenministeriums beziehen – unzutreffend. Eine Ankündigung zum Inhalt der Rede Herrn Mildes am 24. Oktober 1990 im Hessischen Landtag – von deren Inhalt die Pressestelle des Hessischen Innenministeriums erst durch die Rede selbst Kenntnis erlangte – hat es durch die Pressestelle des Innenministeriums nicht gegeben.

17.2.3
Bericht des Hessischen Datenschutzbeauftragten vom 19. November 1990 auf Beschluß des Hauptausschusses vom 8. November 1990

1. Auftrag

Der Hauptausschuß des Hessischen Landtags hat in seiner Sitzung vom 8. November 1990 folgenden Beschluß gefaßt:

Die Landesregierung wird um einen Bericht über den Umgang mit Informationen, die aus Telefonüberwachungsmaßnahmen gewonnen wurden, innerhalb der Landesregierung ersucht, der dem Ausschuß in Verbindung mit einer Stellungnahme des Datenschutzbeauftragten vorgelegt werden soll.

2. Bericht der Landesregierung

Minister Koch hat mir am 14. November 1990 in Erfüllung dieses Auftrags einen Bericht der Landesregierung zugeleitet. Wegen des Sachverhalts, d.h. der Anordnung der Telefonüberwachungsmaßnahme im November 1990, deren Durchführung und der Weiterleitung von Informationen und Abhörprotokollen durch das Bundeskriminalamt an die Staatsanwaltschaft in Frankfurt/Main, die Kriminalpolizei in Frankfurt/Main und von dort an das Hessische Ministerium des Innern, nimmt der Bericht Bezug auf meine Stellungnahme vom 8. November 1990 an den Hauptausschuß. Er betont, daß die in meinem Bericht getroffenen Feststellungen, soweit sie den Sachverhalt betreffen, mit den Erkenntnissen der Landesregierung übereinstimmen.

Darüber hinaus enthält der Bericht der Landesregierung:

a) einen Bericht des Chefs der Staatskanzlei

- über die ihm von Minister Milde zugeleiteten Informationen und deren weitere Verwendung in einem Gespräch mit dem Chefredakteur der Zeitschrift „STERN";

- über vorbereitende Gespräche für die Aktuelle Stunde des Hessischen Landtags am 24. Oktober 1990
  - zwischen dem Chef der Staatskanzlei und dem Ministerpräsidenten;
  - zwischen dem Chef der Staatskanzlei, dem Innenminister und dem Frankfurter Polizeipräsidenten und schließlich

- über eine Besprechung am Nachmittag des 22. Oktober 1990 im Privathaus von Minister Milde in Darmstadt, an der neben dem Innenminister der Ministerpräsident, der Chef der Staatskanzlei, der Büroleiter des Ministerpräsidenten, der Regierungssprecher und der Sprecher der CDU-Fraktion teilnahmen.

  Der Bericht der Staatskanzlei wird durch dienstliche Erklärungen des Sprechers der Landesregierung sowie des Leiters des persönlichen Büros des Ministerpräsidenten ergänzt.

b) eine Stellungnahme des Staatssekretärs beim Hessischen Ministerium des Innern und

c) eine Stellungnahme des Pressesprechers des Hessischen Ministeriums des Innern.

3. Maßnahmen zur weiteren Aufklärung des Sachverhalts

3.1
Zur weiteren Aufklärung des Sachverhalts habe ich zunächst Gespräche mit der Staatsanwaltschaft bei dem Landgericht Frankfurt/Main sowie dem Polizeipräsidium Frankfurt/Main geführt.

Die Vertreter des Polizeipräsidiums haben erklärt, es habe keinerlei direkte Kontakte der Beamten mit Dienststellen der Hessischen Landesregierung, Abgeordneten im Parlament, Vertretern politischer Parteien oder der Medien gegeben, mit Ausnahme der bereits in meinem Bericht vom 8. November 1990 erwähnten Unterrichtung des Hessischen Innenministeriums.

Polizeipräsident Dr. Gemmer hat sein im Bericht der Landesregierung erwähntes Gespräch bestätigt und ausdrücklich betont, daß dabei von dem abgehörten Telefongespräch keine Rede war. Außerdem wies er darauf hin, zum damaligen Zeitpunkt sei ihm die Abhörmaßnahme nicht bekannt gewesen.

3.2
In der Fernsehsendung „Parlament, Parteien, Perspektiven" des Hessischen Rundfunks am 14. November 1990 wurde ein mir inzwischen vorliegendes Schreiben der „STERN"-Chefredaktion, unterzeichnet von Herrn Michael Seufert, an den Hessischen Rundfunk gezeigt. Dieser Brief nimmt Bezug auf das Telefongespräch zwischen dem Chef der Staatskanzlei und dem Chefredakteur des „STERN", Herrn Schmidt-Holtz. Das Schreiben enthält eine Erklärung von Herrn Schmidt-Holtz, nach der Herr Dr. Gauland auf die Frage nach der Quelle der Informationen mitgeteilt habe, es seien „Erkenntnisse über ein Telefongespräch".

Ich habe daraufhin Herrn Schmidt-Holtz angerufen. Er bestätigte, daß nach seiner Erinnerung Herr Dr. Gauland die Formulierung „Erkenntnisse über ein Telefongespräch" gebraucht habe. Zu weiteren Einzelheiten wollte er sich nicht äußern.

Mir gegenüber hat Herr Dr. Gauland diese Darstellung des „STERN"-Chefredakteurs ausdrücklich bestritten.

4. Datenschutzrechtliche Bewertung

4.1
Der Bericht der Landesregierung gibt Anlaß zur datenschutzrechtlichen Bewertung folgender Vorgänge:

- der Weiterleitung der aus der Zusammenfassung des Abhörprotokolls gewonnenen Informationen durch Minister Milde an den Chef der Staatskanzlei;

- der Weiterverwendung dieser Informationen durch den Chef der Staatskanzlei gegenüber dem Chefredakteur des „STERN", Schmidt-Holtz;

- der Mitteilung der Minister Milde vorliegenden Informationen an die Teilnehmer der vorbereitenden Sitzung am 22. Oktober 1990;

- der Verwendung dieser Informationen durch den Pressesprecher des Hessischen Ministeriums des Innern am 24. Oktober 1990;

- der Erklärung des Staatssekretärs beim Hessischen Ministerium des Innern.

4.2
Verwendung der Informationen aus der Telefonüberwachung durch Minister Milde gegenüber dem Chef der Staatskanzlei und in der Sitzung vom 22. Oktober 1990

Wie ich bereits in meinem Bericht vom 8. November 1990 ausgeführt habe, durften die im Rahmen der Telefonüberwachung gewonnenen Erkenntnisse grundsätzlich nur zweckgebunden, d.h. in einem konkreten Zusammenhang mit der Strafverfolgung genutzt werden. Angesichts des besonderen Schutzes des Fernmeldegeheimnisses nach Art. 10 GG und der restriktiven Bestimmungen von §§ 100a, 100b StPO, die einen solchen Eingriff ausschließlich zur Verfolgung bestimmter, besonders schwerwiegender Straftaten zulassen, durfte die Zusammenfassung des Abhörprotokolls nicht unter Berufung auf die angeblich bestehende Fach- oder Dienstaufsicht ohne Kenntnis der Staatsanwaltschaft an den Minister weitergeleitet werden.

Ebenso wie die Offenlegung dieser Informationen durch Minister Milde an das Parlament stellt die Weitergabe an den Chef der Staatskanzlei einen weiteren Eingriff in das Fernmeldegeheimnis dar. Dabei kommt es nicht darauf an, daß das Protokoll selbst nicht übergeben wurde oder ein ausdrücklicher Hinweis auf die Herkunft der Informationen nicht erfolgte. Nach den Maßstäben des von mir bereits im Bericht vom 8. November 1990 zitierten Urteils des Hamburgischen Verfassungsgerichts (NJW 1989, 1081) fehlte es an einer besonderen gesetzlichen Grundlage für die weitere Verwendung der Kenntnisse aus der Telefonüberwachung gegenüber dem Chef der Staatskanzlei.

Die Unzulässigkeit der Weitergabe ergibt sich darüber hinaus aus § 19 Abs. 4 des Hessischen Datenschutzgesetzes. Danach muß eine rechtswidrig erlangte Information gelöscht werden; jede Weiterverwendung, insbesondere deren Übermittlung ist untersagt.

Soweit Minister Milde den Teilnehmern an der Sitzung am 22. Oktober 1990 Informationen aus der Telefonüberwachung mitteilte, gilt die gleiche Bewertung.

4.3
Verwendung der Informationen durch den Chef der Staatskanzlei gegenüber dem Chefredakteur Schmidt-Holtz

Minister Milde hat dem Chef der Staatskanzlei die Informationen aus der Telefonüberwachung rechtswidrig übermittelt (Ziff. 4.2). Rechtswidrig erlangte Informationen dürfen gemäß § 19 Abs. 4 HDSG nicht weiterverwendet werden. Dieses Verwertungsverbot kann allerdings nur greifen, soweit der Empfänger die Rechtswidrigkeit der Übermittlung kennt oder Zweifel an der Rechtmäßigkeit haben mußte. In letzterem Fall ist der Empfänger verpflichtet, von sich aus zu versuchen, die Zweifel an der Rechtmäßigkeit zu beheben. Entscheidend ist also, ob für den Chef der Staatskanzlei im konkreten Fall eine solche Prüfpflicht bestanden hat.

Die Antwort auf diese Frage hängt vom Sachverhalt ab. Mir liegen zwei unterschiedliche Darstellungen zum Inhalt des Telefongesprächs zwischen dem Chef der Staatskanzlei und dem Chefredakteur des „STERN" vor. Mit den mir zur Verfügung stehenden Mitteln kann ich nicht aufklären, wie das Gespräch tatsächlich verlaufen ist. Ich muß daher beide Versionen alternativ bewerten.

a) In seinem Bericht weist der Chef der Staatskanzlei darauf hin, daß es der Innenminister ausdrücklich abgelehnt habe, die Herkunft seiner Informationen offenzulegen. Dies entspricht der Darstellung, die Minister Milde mir gegenüber im Zusammenhang mit meinem ersten Bericht gegeben hat.

   Einerseits könnte man sich in Anbetracht der Weigerung von Minister Milde die Informationsquelle zu nennen, fragen, ob dies nicht für den Chef der Staatskanzlei ein ausreichender Anlaß hätte sein müssen, sich noch einmal explizit danach zu erkundigen und bei einer wiederholten Verweigerung von der Verwendung der Mitteilung

abzusehen. Andererseits ist zu berücksichtigen, daß diese Äußerung vom Innenminister kam, der, ebenso wie etwa der Justizminister, aufgrund seiner Funktion eine besondere Verantwortung für die Rechtmäßigkeit der Verarbeitung personenbezogener Informationen trägt. Nimmt man hinzu, daß verschiedene legitime Motive denkbar sind, aus denen der Innenminister keine Angaben über die Quelle der Informationen machen wollte, bestand meines Erachtens kein Anlaß für eine Rückfrage. In diesem Zusammenhang ist auch zu berücksichtigen, daß die Funktionsfähigkeit eines Kabinetts ein bestimmtes Maß an gegenseitigem Vertrauen voraussetzt.

Deshalb bestand unter diesen Voraussetzungen für den Chef der Staatskanzlei keine Prüfpflicht.

b) Folgt man der vom Chefredakteur des „STERN" gegebenen Version, hat der Chef der Staatskanzlei im Telefonat mit ihm auf die Frage nach der Quelle seiner Information von „Erkenntnisse(n) über ein Telefongespräch" gesprochen. Die Formulierung ist nicht eindeutig. Es ist nicht aufklärbar, um welches Telefonat es sich gehandelt haben könnte. Nur eine der denkbaren Möglichkeiten ist es, daß Dr. Gauland diese Formulierung wählte, weil ihm die Herkunft der Mitteilung aus einem abgehörten Ferngespräch bekannt war. In diesem Fall wäre er verpflichtet gewesen, sich vor jedem Gebrauch der Information über die Zulässigkeit der Verwendung zu vergewissern. Wären die Zweifel nicht zu beseitigen gewesen, hätte er die Mitteilung an Dritte unterlassen müssen.

4.4
Verwendung der Informationen durch den Pressesprecher des Ministeriums des Innern

Der Pressesprecher des Ministeriums des Innern erklärt, er habe lediglich eine Presseerklärung verfaßt und zwar aufgrund der Debatte im Landtag nach Auswertung des Redebeitrages von Minister Milde.

Aus dieser Angabe ergeben sich keine Anhaltspunkte für einen Verstoß gegen das Datenschutzrecht.

4.5
Kenntnisnahme durch den Staatssekretär beim Hessischen Ministerium des Innern

Nach der Darlegung des Staatssekretärs beim Hessischen Ministerium des Innern hat dieser von der Existenz der Zusammenfassung des Abhörprotokolls am Vortag der Aktuellen Stunde im Landtag, von dem Inhalt hingegen erst durch die Rede von Minister Milde erfahren.

Daraus läßt sich, soweit es um den Staatssekretär geht, jedenfalls kein Verstoß gegen datenschutzrechtliche Bestimmungen entnehmen.

5. Weitere Konsequenzen

In meinem ersten Bericht vom 8. November 1990 habe ich auf eine Reihe notwendiger Konsequenzen hingewiesen. Dabei hatte ich hervorgehoben, daß es ganz besonders darauf ankommt, das Verhältnis zwischen polizeilicher Fach- und Dienstaufsicht und staatsanwaltschaftlicher Sachleitungsbefugnis rasch zu klären. Wie berechtigt diese Forderung ist, haben meine jüngsten Gespräche in der letzten Woche mit Vertretern der Staatsanwaltschaft und des Polizeipräsidiums in Frankfurt/Main ergeben:

So betonte der Stellvertretende Leiter der Staatsanwaltschaft Frankfurt/Main noch einmal ausdrücklich, neben der Sachleitungsbefugnis der Staatsanwaltschaft gebe es keinen Raum für fachaufsichtliche Maßnahmen durch das Hessische Ministerium des Innern. Eine Weitergabe von Abhörprotokollen oder Informationen aus diesen bedürften in jedem Fall der Zustimmung durch die Staatsanwaltschaft.

Demgegenüber vertraten leitende Mitarbeiter des Polizeipräsidiums in Frankfurt/Main die Ansicht, daß nicht nur dienst-, sondern auch fachaufsichtliche Maßnahmen durch vorgesetzte Dienststellen einschließlich des Ministeriums des Innern zulässig seien, selbst wenn im konkreten Fall die Staatsanwaltschaft ihre Sachleitungsbefugnis wahrnehme. Dies schließe die Verwendung von Abhörprotokollen aus der Telefonüberwachung ein.

Diese Auffassung findet sich auch in der Stellungnahme vom 16. November 1990 der Fachabteilung III (Polizei) des Hessischen Ministeriums des Innern zu meinem ersten Bericht. Ohne in diesem Bericht auf Einzelheiten der Stellungnahme einzugehen, steht soviel fest: Selbst wenn man sich dem dort vertretenen Rechtsstandpunkt anschließen würde, ist nicht zu erkennen, daß die Information aus dem abgehörten Telefongespräch in irgendeiner Weise für die Dienst- und Fachaufsicht erforderlich sein konnte.

Ich unterstütze die Anregung von Minister Koch, eine Arbeitsgruppe aus Vertretern des Landtags und der Landesregierung unter Beteiligung des Hessischen Datenschutzbeauftragten zu bilden, um für die Zukunft die notwendigen verfahrensrechtlichen Vorgaben zu formulieren. Dort wird das Hessische Ministerium der Justiz sicherlich seine Rechtsauffassung zu den Positionen von Polizei und zuständiger Fachabteilung des Innenministeriums darlegen.

17.3
Beschlüsse und Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz

17.3.1
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Bundesdatenschutzgesetz vom 22./23. März 1990 und zum Bundesverfassungsschutzgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz (gegen die Stimme Bayerns) begrüßt die mit den am 13. März 1990 vorgelegten Vorschlägen der Koalitionsfraktionen verbundene Absicht, die längst fällige Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes noch rechtzeitig vor dem Ende der Legislaturperiode zu verabschieden.

Die Vorschläge zum Bundesdatenschutzgesetz beseitigen eine Reihe von Schwächen des Regierungsentwurfes. Hervorzuheben ist insoweit

- daß nunmehr für den öffentlichen Bereich die Verarbeitung personenbezogener Daten in Akten und die Datenerhebung durch öffentliche Stellen in den Geltungsbereich des Bundesdatenschutzgesetzes einbezogen werden,

- daß künftig der Bundesbeauftragte für den Datenschutz durch das Parlament gewählt werden soll,

- daß der Betroffene bei Ablehnung der Auskunftserteilung darauf hingewiesen wird, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

Demgegenüber weisen auch die Vorschläge noch Schwächen und Defizite auf. Dazu gehören u.a.

- die unzureichende Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei der Datenverarbeitung in Akten,

- ein Widerspruchsvorbehalt für die Betroffenen gegen eine Kontrolle ihrer Daten durch den Bundesbeauftragten für den Datenschutz, der systematische Prüfungen gefährdet und deshalb entbehrlich ist, weil es für die Datenschutzbeauftragten schon immer selbstverständlich war, die Daten von Betroffenen nicht gegen deren erklärten Willen in Kontrollen einzubeziehen,

- die verfassungswidrige Erstreckung des Widerspruchsvorbehaltes in der Neufassung auf die Landesbeauftragten für den Datenschutz,

- das Fehlen eines gesonderten Gesetzesvorbehaltes für die Einrichtung von Direktzugriffsverfahren in besonders sensiblen Bereichen,

- der zu weite Katalog erlaubter Zweckänderungen und die unzureichende Unterrichtung des Betroffenen über die Zweckänderung.

Im Bereich der Datenverarbeitung durch nichtöffentliche Stellen verschlechtern einzelne vorgeschlagene Regelungen die Rechte der Betroffenen im Vergleich zum geltenden Gesetz, etwa bei der Übermittlung von Daten an den Adressenhandel. Sie bleiben im übrigen weit hinter den Vorschlägen für den öffentlichen Bereich zurück. Weder die Verarbeitung der Akten noch die Datenerhebung werden einbezogen. Auch die höchst unzureichenden Kontrollbefugnisse der Datenschutzaufsichtbehörden sind nicht wesentlich verbessert worden.

Schließlich erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie von Regelungen für den Kredit- und Versicherungsbereich.

Zu den Vorschlägen der Koalition für das Bundesverfassungsschutzgesetz stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Vorschläge bringen gegenüber dem Vorentwurf der Bundesregierung Verbesserungen. Dies gilt insbesondere für

- den Schutz des in Wohnungen nichtöffentlich gesprochenen Wortes vor heimlichem Mithören und Aufzeichnen,

- die Einschränkung der Speicherung von Daten über Minderjährige,

- die konkretisierenden und einschränkenden Regelungen für den Einsatz nachrichtendienstlicher Mittel,

- die präzise Definition der „Bestrebungen" gegen die freiheitlich-demokratische Grundordnung,

– die Anknüpfung der Sammlung und Verarbeitung von Daten an das Vorliegen tatsächlicher Voraussetzungen.

Hingegen sind u.a. folgende datenschutzrechtliche Anforderungen noch nicht erfüllt:

– Die Befugnisse zur Datenverarbeitung müssen differenziert den unterschiedlichen Aufgaben zugeordnet werden.

– Die Datenspeicherung ist nicht so präzise geregelt, daß der Bürger dem Gesetz entnehmen kann, unter welchen in seiner Person liegenden Voraussetzungen der Verfassungsschutz über ihn Daten speichern darf.

– Die Zweckbindung der Daten innerhalb des Verfassungsschutzes ist nicht gewährleistet.

– Das Auskunftsrecht des Bürgers auch gegenüber den Verfassungsschutzbehörden wird zwar nunmehr erstmals anerkannt. Die vorgeschlagene Regelung schränkt aber den Auskunftsanspruch zu sehr ein. So wird dem Bürger eine Pflicht zur Begründung seines Auskunftsersuchens auferlegt, während die Ablehnung der Auskunft unter keinen Umständen begründet werden muß.

– Die vorgesehenen Regelungen zur Sicherheitsüberprüfung ersetzen nicht eine bereichsspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren.

Die Datenschutzbeauftragten gehen davon aus und halten es für notwendig, daß die bestehenden Mängel der Gesetzentwürfe in den anstehenden Parlamentsberatungen behoben und ihre Anregungen aufgegriffen werden.

17.3.2
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis

1.
Das Engagement der Bevölkerung der DDR für den Schutz ihrer personenbezogenen Daten z.B. beim Staatssicherheitsdienst zeigt, wie elementar die Persönlichkeitsrechte von den Bürgern in der DDR verstanden werden und daß sie das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Selbstbestimmungsrechts wahrnehmen.

Die Konferenz der Datenschutzbeauftragten begrüßt Bemühungen, auch in der DDR angemessene Datenschutzregelungen zu schaffen.

2.
Obwohl in der DDR keine hinreichenden Datenschutzregelungen bestehen, werden bereits jetzt mehr personenbezogene Daten als früher ausgetauscht. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen, sowie im Rahmen der Gefahrenabwehr und der Strafverfolgung haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitendem Datenverkehr, z.B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschutzes auf. Für die Bundesrepublik gelten das allgemeine Datenschutzrecht und besondere Gesetze, wie z.B. das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 sowie Vereinbarungen.

Bei der Verwirklichung technischer Maßnahmen inbesondere bei dem Ausbau der Telekommunikationsdienste und bei der automatisierten Datenverarbeitung muß der Datenschutz beachtet werden.

3.
Die Datenschutzkonferenz hält es für geboten, daß der Austausch personenbezogener Daten zwischen Behörden und öffentlichen Stellen in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik erst durchgeführt wird, wenn gewährleistet ist, daß nach folgenden Grundsätzen verfahren wird:

– Die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 sind zu beachten.

– Die Übermittlung personenbezogener Informationen unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines Gesetzes der Bundesrepublik Deutschland verstoßen würde oder schutzwürdige Belange bei den betroffenen Personen beeinträchtigt würden. Die Übermittlung personenbezogener Informationen unterbleibt insbesondere dann, wenn Grund zu der Annahme besteht, daß die Verwendung der übermittelten Informationen nicht in Einklang mit rechtsstaatlichen Grundsätzen steht oder dem Betroffenen aus der Verwendung der Informationen erhebliche Nachteile erwachsen, die im Widerspruch zu rechtsstaatlichen Grundsätzen stehen.

- Der Empfänger darf personenbezogene Informationen nur zu dem durch die übermittelnde Stelle angegebenen Zweck und unter den von ihr vorgeschriebenen Bedingungen nutzen.

- Personenbezogene Informationen dürfen ausschließlich an die in den Abkommen oder Absprachen genannten Behörden übermittelt werden. Eine Übermittlung an andere Stellen darf nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.

- Der Empfänger unterrichtet die übermittelnde Stelle und den zuständigen Datenschutzbeauftragten auf Ersuchen über die Verwendung der übermittelten Informationen und über die dadurch erzielten Ergebnisse.

- Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Informationen zu achten. Erweist sich, daß unrichtige oder zu vernichtende personenbezogene Informationen übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Dieser ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.

- Dem Betroffenen ist auf Antrag über die zu seiner Person vorhandenen Informationen sowie über den vorgesehenen Verwendungszweck Auskunft zu erteilen. Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit eine Abwägung ergibt, daß eine Auskunft den Verwendungszweck oder schutzwürdige Interessen Dritter gefährden würde.

- Die Übermittlung und der Empfang personenbezogener Informationen sind aktenkundig zu machen.

- Zur Gewährleistung dieser Grundsätze sind die verfahrensmäßigen Sicherungen vorzusehen. Dazu kann es gehören, besondere Stellen mit der Datenübermittlung zu beauftragen. Die Kontrolle der Datenübermittlung durch unabhängige Datenschutzbeauftragte muß gewährleistet sein.

4.
Die Verarbeitung personenbezogener Daten bei den Sicherheitsbehörden der Bundesrepublik Deutschland muß im Hinblick auf die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa über die bereits getroffenen Maßnahmen hinaus überprüft werden. Diese Notwendigkeit besteht u.a. bei

- dem Verfahren der Sicherheitsüberprüfung,

- der Datenerhebung und Datenübermittlung des Bundesgrenzschutzes anläßlich von Grenzkontrollen an die Nachrichtendienste,

- der Bereinigung der Datensammlungen der Verfassungsschutzbehörden.

17.3.3
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zur Einrichtung eines Arbeitskreises EG

1.
Der Arbeitskreis EG (AK EG) hat die Aufgabe, zum frühestmöglichen Zeitpunkt Informationen über Entwürfe, Vorschläge und Projekte der EG-Organe und des Europarats mit datenschutzrelevantem Inhalt zu beschaffen und diese umgehend allen Datenschutzbeauftragten zuzuleiten. Der AK EG verfolgt die weitere Behandlung dieser Vorhaben in den Institutionen auf EG/Europarats-Ebene sowie auf Bundes- und Landesebene (Bundesrat).

2.
Zu den unter 1. genannten Aufgaben knüpft bzw. koordiniert der AK EG Kontakte zu den mit Datenschutzfragen befaßten Institutionen und Personen auf den Ebenen EG, Europarat, Bundesregierung, Bundestag(sfraktionen), Bundesrat, Landesregierungen usw. Gleiches gilt für die Datenschutzinstitutionen in den EG-Nachbarländern.

3.
Der AK EG hält Kontakt zur Arbeitsgruppe „Internationaler Datenverkehr" des Düsseldorfer Kreises und lädt im Regelfall einen ihrer Vertreter zu seinen Sitzungen ein.

4.
Vorhaben, die in den Aufgabenbereich eines bestehenden Arbeitskreises der DSB-Konferenz gehören, werden inhaltlich dort behandelt. Soweit dies nicht der Fall ist, insbesondere bei übergreifenden oder Querschnittsthemen (z.B. Entwurf einer Rahmenrichtlinie zum Datenschutz in der EG), werden diese im AK EG behandelt.

5.
Der Vorsitz des AK EG wechselt jährlich. Im ersten führt der Hessische Datenschutzbeauftragte (HDSB) den Vorsitz. Im darauffolgenden Jahr wird der Vorsitz vom Bundesbeauftragten (BfD) wahrgenommen. Je ein Mitarbeiter von BfD und HDSB bilden gemeinsam das „Sekretariat" des AK EG.

17.3.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 27. Juni 1990 zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauschgifthandels und sonstiger organisierter Kriminialität – die im übrigen nicht definiert wird –, sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtlichen Bedenken:

- Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung des Gesetzentwurfs in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z.B. auch die Rasterfahndung für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich miteinbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.

- Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig. So dürfen ohne Wissen des Betroffenen zur Aufklärung jeder Straftat – sogar in Wohnungen hinein – „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.

- Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte unverdächtige Personen richten, wenn „aufgrund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.

- Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.

- Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige richterliche Kontrolle zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z.B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

17.3.5
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß frühzeitig begegnet werden:

- Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.

- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z.B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.

- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z.B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich,

- die gesetzlichen Regelungen präziser und enger zu fassen,

- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,

- erlaubte Eingriffe in das Grundrecht nach Art. 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen.

- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z.B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

Enthaltung: Bayern

17.3.6
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes

Der dem Deutschen Bundestag vorliegende Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes hält weiter an der Hotel- und Krankenhausmeldepflicht fest. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat erhebliche Bedenken, ob dem Bund die Gesetzgebungskompetenz zur Regelung dieser Frage zusteht. In jedem Fall ist zu bedenken:

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr ist zu berücksichtigen, daß es sich im Regelfall um Bürger handelt, die ein Recht darauf haben, von polizeilichen Ermittlungen unbehelligt zu bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz ist darüber hinaus der Auffassung, daß den Bürgern in allen Meldegesetzen ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeräumt werden muß.

Gegenstimme Bayern mit Ausnahme des letzten Absatzes.

17.3.7

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern

1.
Die Datenschutzbeauftragten haben schon in ihren Entschließungen vom 14. Dezember 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag des Datenschutzbeauftragten, darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.

2.
Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Art. 1 i.V.m. Art. 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-Patienten-Verhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt.

Sie sind nach wie vor der Meinung, daß das Krebsregister nur mit Einwilligung von Patienten oder auf anonymer Basis geführt werden kann. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sie in Erwägung zu ziehen.